Cyber security of national critical infrastructure in Geo-political conflicts .

Pratik Suryakant Pawar
Master Of Science (Information Technology)
Ramnarain Ruia Autonomous College
pratikpawar0222@gmail.com

Abstract :
This paper examines security threats of national critical infrastructure during geopolitical tensions with a focus on the telecommunications sector of India. This evaluates how newer , modern events including the disruption of Ukraine's telecoms network challenge the conventional approaches to security. In order to solve the problems and needs , this paper presents the integration and suggestion of blockchain technology to improve security and resiliency . Thus, using private blockchain solutions like Hyperledger Fabric and the Lightning Network, as well as Schnorr signatures, this solution intends to supply a stronger and more resilient protection against cyber risks. The paper analyses the possibilities of application and benefits of these technologies to protect the telecommunications of India.

Introduction :
As the world is turning into the digital world and is getting interconnected , the importance of protecting and securing National Critical Infrastructure (NCI) has become vital particularly with increasing Geopolitical tensions. National Critical Infrastructure (NCI) means essential infrastructures , assets and data networks which are necessary for the nation's functioning . The protection of national critical infrastructure is steadily turning into one of the major pillars of national security. This topic is becoming apparent for the reason that the threat of cyberattacks is constantly growing and progressing and has negative impacts on national security, and can lead to severe consequences for national security, economic stability, and public safety and can cause widespread societal and economic damage.

National Critical Information Infrastructure Protection Centre (NCIIPC) India , has recognized 7 major infrastructures/sectors as critical infrastructure that includes : Banking, Financial Services, and Insurance(Bfsi), Health , S&PE , Government , Transport ,Power and Energy , Telecom .

This study examines cybersecurity threats to India's national critical infrastructure, particularly a closer examination of the telecommunications infrastructure— the telecommunications infrastructure not only facilitates communication networks, but is also integral to delivery of other important services such as emergency services, financial systems, and military operations.

This research will also provide important insights into how cyber attacks in geopolitical situations can threaten national critical infrastructure.

In the present day, a secure communications infrastructure is just as critical to a nation's safety as its physical borders and the key importance of this study can be attributed to the timeliness and relevance of the current geopolitical environment in India. State sponsored risks to critical infrastructure have significantly increased as relations with China and Pakistan continue to deteriorate. Cyber actors will therefore consider telecommunication infrastructure as an appealing target to facilitate creating harm and destabilise the nation states while having a significant reliance on civilian and militarily based operational communications. This study will examine the specific risks and vulnerabilities of India's telecommunication sector outside of the political aspect of a geopolitical ecosystem. Specifically addressing how cyber attacks, in particular the more frequently occurring Distributed Denial of Service (DdoS) attacks can impair communications overall. In addition, it will affect all services that are considered critical in delivering operational effectiveness and efficient delivery of resources. By understanding the specific risks and providing cybersecurity related recommendations, including threat assessments for DDoS mitigation this research will provide and suggest possible solutions that might contribute to sustaining or improving cyber resilience.

This paper is based on recent case studies and governmental reports and documents. It reviews the trends in how cyber threats evolve, especially DDoS attacks that have been used for targeting telecommunications networks.

Recognising that a lot of research has been conducted on global cybersecurity, there is still an important lack of studies that focus on vulnerabilities of India's telecommunications sector in this specific geopolitical context. The research presented in this study is an attempt to provide that informed gap by documenting various cyber threats particularly Distributed Denial of Service (DDoS) attacks.

The originality and creativity of this research derives from the proposed integrated approach that combines geopolitical analysis with advanced technological solutions for India's telecommunications industry. Identifying past cyberattacks aimed at India's telecom infrastructure and also other nations telecom infrastructure , exploring advanced technologically derived solutions such as blockchain , and DDoS mitigation strategies; while providing actionable solutions that aim to enhance the resilience of India's critical infrastructure.

In conclusion, this research seeks to provide a layered understanding of the cybersecurity challenges faced by India’s telecommunications infrastructure and also showcasing the dynamic connection within geopolitics, technological advancements, and national security. As a result, this research serves to inform strong adaptive solutions to the protection of India's critical telecommunications networks in an increasingly interconnected and unpredictably volatile digital world.

Methodology :

This research is designed to conduct through mixed methods (qualitative and quantitative), thereby giving an in depth account of this issue. The mixed method analysis offers a greater potential to investigate the complex nature of online cyber threats in more detail.
The objective of this research is to explore the issues of cybersecurity challenges faced by national critical infrastructure in India through the lens of the telecommunications industry as it relates to increasing geopolitical tensions. This research will identify vulnerabilities, assess the impact of the threat of cyber threats (especially Distributed Denial of Service DDOS attack) and examine applied methods for improving cybersecurity resilience.

Questions:

1. Why is telecommunication infrastructure essential to India's economy and national security?

2. What types of attacks present the most significant cybersecurity threats to India's telecommunication infrastructure during geopolitical conflict?

3. How can Pakistan , China and any other country can leverage attacks on India's telecommunication infrastructure during geopolitical tension, to India's detriment?

4. How can DDoS attacks be a weapon during geopolitical tensions?

5. To what degree does telecommunications interdependence with other critical infrastructures amplify the DDoS risk of geopolitical conflict exploring other critical services (e.g. energy, finance)?

6. Does a decentralised blockchain system offer better DDoS attack aversion over centralised infrastructure vulnerabilities? .

7. Can blockchain technology effectively enhance the resilience of India's telecommunications infrastructure against DDoS attacks?

8. What are the advantages of using blockchain technology to secure India's telecommunication infrastructure (security, transparency, accountability)?

9. How effective are our current cybersecurity measures to prevent DDoS attacks on India's telecommunication infrastructure?

10. What are the cybersecurity measures that telecom companies deploy to mitigate DDoS attacks that are widely adopted?

11. What barriers and limitations exist in implementing blockchain technology in the telecom industry?

Sampling Strategy utilised voluntary sampling to select relevant case studies, of significant cyberattacks on telecommunications infrastructure including the Ukraine telecommunications disruption , due to the applicability in illustrating potential risks to India.

Data Collection involved qualitative analysis of governmental reports, cybersecurity white papers, cybersecurity agencies papers , alongside quantitative analysis of cybersecurity incident databases to determine the frequency and impact of DDoS attacks.

Data Analysis was conducted using a Quantitative approach, which involved analysing data statistically to understand the frequency and impact of DDos attacks. Qualitative data was analysed thematically to identify common vulnerabilities and effective mitigation strategies .

The current research also considers its shortcomings, such as using secondary sources of information from the internet and focusing on a specific geopolitical context , which can limit the scope of the results.

Results :

This study involves the cyber risks to national critical infrastructure, with specific emphasis on the telecommunications sector in India. The study draws on offensive cyber events around the world, specifically the disruptions in Ukraine to its telecommunication systems, and examines the types of attacks that could result in similar disruption in India. Blockchain based methods for improving national cyber resilience are presented in the discussion section..

With regards to the quantitative data that has been taken and compiled relating to the extent of cyberattacks against national critical infrastructure around the globe, between January 2023 and January 2024, there were over 420 million cyberattacks against global critical infrastructure or approximately 13 attacks per second. This increase was up by 30 percent from last year. There were attacks against national critical infrastructure in 163 countries, with attacks against the United States of America , United Kingdom , Germany, India and Japan leading other nations. Cyberattacks from China, Russia and Iran remained the sovereign nations with the leading attacks.

With statistical data indicating the number of DDoS attacks against critical national infrastructure for the previous years, it noted a 47 percent year on year increase, with government services being the most targeted area representing 34 percent of all attacks. The DDoS attacks were determined and reported to have increased, in part due to geopolitical events, including elections in 64 countries. In 2023, the DDoS attacks continued to grow, feeding into more high frequency automated increases, and more advanced attacks with increased multivector attacks, along with growing the average numbers of devices upon attack networks. The average increase is reported to reach a fivefold increase , increasing the botnet average of devices involved in reported events from 4,000 to 20,000 on its device network with reported DDoS attacks against critical infrastructure, including DNS services. The DDoS attacks have consistently remained heightened, including reporting over 13

million reported events in 2022 alone, which was a record high for DDoS incident rates. The average attack rates were continuing to increase in numbers, with many of now sustained attacker campaigns of over 20 minutes in time, and increased by 50 percent for attacks exceeding one hour. between 20212023. The reported events in 2023 indicated the DDoS attacks doubled from the prior year in 2022 which indicated an overall growth of 112 percent. The telecommunications sector specifically to DDoS frequency and incident reporting increased by fivefold as part of notable sector ranges of services to be exploited by threat actors, organised crime and cybercriminals. Overall, the telecommunications sector has been highlighted since 2021 as being one of the most targeted, along with software and computer services.

During April 2023, a large set of DDoS attacks targeted multiple major Indian airports and healthcare institutions, exposing the vulnerability of critical infrastructures, including telecommunications, to cyber threats.

In Q1 2024, there was a global increase in DDoS attacks by 50% year over year with hacktivist groups targeting geopolitical actors, including India. Government services suffered the highest percentage of attacks, which accounted for 34% of the monthly incidents. This increase in DDoS attacks was part of a general increase in attack rates during election cycles around the world, such as India,

The average organisation faced 11 attacks per year, implying many companies must contend with attacks almost monthly. The biggest attack recorded in 2023 peaked at an astonishing 1 Tbps (1 Tbps means 1 terabytes of requests were made per second), highlighting the increasing scale of these threats worldwide.

An average cost that company or nation can expect when a DDoS attack takes place is considerable. Multiple studies inhabit a possibility space of financial costs:

Average Downtime Costs : The Ponemon Institute calculates that the average loss of a minute of downtime, as the result of a DDoS attack, is roughly $22,000. The average attack lasts 54 minutes, the average total loss, due to DDoS attacks is, therefore, about $1.188 million per attack.

Hourly Costs: Possible values from other studies suggest that businesses , especially large organisations, in the finance and ecommerce sectors; hourly losses in some cases are $300,000 to $1 million (or greater) losses per hour.

Downtime Due to Service Inaccessibility: Average duration of DDoS attacks has increased; some attacks as noted can last 30 minutes or longer, and some are more difficult to even assess attack lengths due prolonged service downtime of the organisation; some attacks have been recorded at lengths of over 50 hours. Longer attacks provide commensurate trajectory increases in financial loss and also operational capacity losses for the organisation in question.

Qualitative Findings :

“Historically, the focus of the telecommunications industry has been on availability and reliability; however, cybersecurity has recently become a greater concern. Organisations must develop a risk based approach and invest in advanced security technologies to maintain a respectable advantage in the industry.”

Before discussing the proposed blockchain-based response, it is valuable to comprehend the available traditional approaches to DDoS mitigation . Standard cybersecurity measures for protecting telecommunication infrastructure generally include:

1. Rate Limiting: Manages the flow of legitimate user traffic to a specific server to avert overload. This approach is effective against volumetric attacks; however, it can inadvertently limit legitimate users during peak traffic.
2. IP Filtering: Disallows or blocks traffic originating from IP addresses known to be malicious. This method can also be effective; however, the database of malicious IP addresses must always be updated, and IP addresses can be difficult to categorise.
3. Blackholing: Below a user-defined threshold, routes all traffic from the source of attack to a null address, which drops the traffic. Although this route effectively eliminates attack traffic, the legitimate traffic drops too, and is not appropriate for an extended attack.
4. Scrubbing Centers: Scrubbing centres analyse the incoming traffic to filter out malicious traffic and allow only legitimate traffic to reach the target server. While this route filters traffic, scrubbing centres can require additional resources and processing time to mitigate DDoS attack traffic.
5. Web Application Firewalls (WAF): A WAF mitigates application layer attacks of HTTP traffic by filtering and monitoring normal traffic for block or allow actions. Like other forms of mitigation, once a WAF is set up improperly, traffic filtering basis may be circumvented.
6. Bot Mitigation Techniques: Various techniques exist that incorporate CAPTCHAs or device fingerprinting to separate bot traffic from human users. Although the use of CAPTCHAs or device fingerprinting help identify bot traffic, legitimate users may experience frustration as a result of unavoidable identification.

At this moment, traditional methods have limitations, especially given the speed and variability of DDoS attacks.

Strengths and capabilities of the telecommunication industry's proactive security measures include several key examples, to reduce and defend against cyberattacks, accidents, and breaches.

1. Multifold layers of defence.

Description: The multiple forms of security is to offer maximum protection of the network.

Vodafone report: Vodafone, in its 2023 security report noted they incorporated a multilayered security approach, reducing successful attacks to the network by 70%, as compared to the previous year.

2. Fast Threat Detection, and response time.

Description: Engaging a security incident event management (SIEM) tools and AI powered branches provides increased detection and response time.

News Report: In 2023 a security report noted that their security service operations centre, engaging AI driven methods to respond to threats and attacks on the network, reduced average response time from 3 hours to 10 minutes.

3. Encryption.

Description: Strong encryption methods can enhance data protection.

Orange, end to end encryption: Orange, in 2022 implemented strong encryption methods, resulting in 99.9% reduction in attack data for their business segment.

4. Network segmentation. In fact this assists with containment.

(need more description).

News Report: AT&T, as noted in the 2023 cybersecurity report, stated that network segmentation contained potential breach to less than 0.1% of networks.

5. Continuous Monitoring and Automated Response

Description: 24/7 monitoring increased chance of detection with automated response capabilities.

Deutsche Telekom report: In 2023 the Deutsche Telekom reached over 1 billion security events monitored each day, 99.99% of which autonomously acted.

6. Information Sharing Agility.

Description: Telecommunication offers opportunities for sharing information. GSMA Report: The GSMA annual report spotlighted shared information and threats, stating enhanced efficiency of approximately 40% reduction based on information sharing.

7. Zero Trust method

Description: assume nothing, and check all incoming information with no trust of the source.

Case study: BT Group provided evidence that its successful delivery to reduce insider threats even further to 60% with the zero trust method implemented into their protocols.

Weaknesses :-

1. Evolving Threat Landscape

Description: Cybercriminals are constantly innovating new attack vectors.

News Story: 5G Network Vulnerabilities

In 2023, the European Union Agency for Cybersecurity (ENISA) published a report that identified 20 new types of attacks on 5G networks,

2. Human Factor :-

Description: Social engineering attacks take advantage of human weaknesses

Case Study: Major Indian Telco Phishing Incident

In 2022, a major Indian Telecom company was breached, impacting over 5 million customers, due a sophisticated phishing attack targeting employees .

3. Legacy Systems

Description: Older systems may not comply with the most recent security requirements.

News Story: UK telecom infrastructure vulnerabilities,

In 2023 a UK government report indicated that 30% of the UK's telecommunications infrastructure relied on legacy systems which have vulnerabilities of unquestionable degree of difficulty .

4. Supply Chain Vulnerabilities :-

Description: Complex supply chains create security vulnerabilities.

Case Study: European 5G Equipment Security Issues.

In 2023, several European countries disclosed that they'd been utilising 5G equipment from a shared, major manufacturer which contained potential backdoors. As a result, each country (England for example) replaced that manufacturer's equipment on a widespread basis.

5. IoT Device Security :-

Description: The large volume of IoT devices creates new attack paths.

News Story: Massive IoT Botnet Attack.

In late 2022, an attack compromised over 1 million devices on an IoT botnet to instigate a Denial of Service attack against numerous European telecommunications providers .

6. Quantum Computing Threat :-

Description: Quantum computers may break the current standard of encryption.

Case Study: Challenges Moving From PostQuantum Cryptography. In 2023, a study by the U.S. National Institute of Standards and Technology (NIST), found that only 12% of telecommunications companies were prepared to move to Quantum Resistant scripting.

7. Regulatory Compliance:-

Description: There are many evolving regulations, and compliance varies.

News Story:- General Data Protection Regulation (GDPR) Telecom Sector Fines :- In 2023, telecommunications companies across Europe faced over €500 million of fines from GDPR, illustrating the challenge to maintain compliance regardless of borders and regions .

Blockchain Solution :-

Introduction:- Distributed Denial of Service (DDoS) attacks represent critical risks to telecommunications infrastructure. They target both government entities and private companies that service the telecom industry. As these attacks become increasingly sophisticated in nature, there is the potential to leverage blockchain technology, and improve resilience, lessen vulnerability, and mitigate the "risks" of DDoS attacks. In this paper, I will

present the potential effectiveness of blockchain-based solutions to mitigate and reduce the "risks" of DDoS attacks and armed conflict when supported through qualitative data with viable case studies.

Potential Effectiveness of Blockchain Solutions

1. Decentralisation and Resilience :- Decentralisation is one of the key benefits of blockchain technology. Decentralised blockchain networks do not have an overarching centre point of failure--unlike many centralised systems do. Centralised systems designate a specific point which operates the system without redundancy from several other points. Blockchain's decentralised nature equally distributes data across many nodes being used. In consequence, if one node of several nodes were attacked during a DDoS Attack, this led to attacks being overwhelmed and pressured, while the overall network would still be running in real time.

Qualitative Data: When evaluating resilience of DDoS attacks there exists evidence that shows extremely decentralised blockchain networks model higher resilience to a DDoS attack than other models. There is no singular which can be taken down or captured rendering the entire systemless at risk of being completely brought down, as one site can simply go offline without affecting the entire network or spreading into larger areas.

2. Improved Security through the use of Immutable Systematic Ledger

Blockchain technology requires that all transactions on its ledger be completed through an immutable systematic ledger. This characteristic improves security through record activity which is more difficult for malicious attacks to alter or even disrupt services.

Qualitative Data: With blockchain providing transactions as being immutable, potential malicious attacks would be deterred from even realising attacking tools in which tampering would require altered events of two-thirds (66%) for changing an immutable transaction. As contextualised, if the blockchain is well-distributed even a DDoS attack would not be able to operationally change the transaction in real-time.

3. Smart Contracts for Automated Defense Mechanisms

Smart contracts can be designed to automatically execute a response as each anomaly is detected, such as sudden spikes in transaction volume, indicating the initiation of a DDoS attack.

Qualitative Data: By deploying smart contracts, telecom operators are able to monitor and respond to attacks, such as rate limiting or blocking suspect IP addresses. The result is reduced impact of the DDoS attack prior to its devastation escalation.

4. Economic deterrents through proof systems

Blockchain networks can use proof of work, or a similar proof mechanism requiring physical computational resources to validate transactions. This economic barrier ensures it is too costly for an attacker to flood the network with fake transactions.

Qualitative Data: The use of proof systems incurs significant expenditures or costs of time and financial resources for executing DDoS attacks; an attacker attempting to launch a denial of service attack, for instance, would require enough physical computation resources for each request to one of these proof systems denoting the trust in transactions.

Limitations and Challenges

While blockchain technology presents significant advantages in mitigating DDoS attacks, it is not without limitations:

1. Transaction Flooding Vulnerability: Blockchain networks can still be susceptible to transaction flooding attacks, where attackers overwhelm the network with fake transactions, filling up the meme pool and delaying legitimate transactions.
2. Resource Intensity: Implementing blockchain solutions, particularly with smart contracts and proof systems, requires considerable computational resources, which may not be feasible for all telecom operators.
3. Complexity of Integration: Integrating blockchain technology into existing telecommunications infrastructure can be complex and may require significant changes to operational processes and systems.
4. Regulatory and Compliance Issues: The use of blockchain in critical infrastructure raises regulatory concerns, particularly regarding data privacy and security compliance. Different jurisdictions may have varying legal frameworks, complicating implementation across regions.

Case Studies and Examples :-

1. Ethereum Network

The Ethereum network underwent two denial of service attacks: the first occurred in 2016 and the second happened in 2022. In both cases, the network experienced an artificial service disruption, proving DDoS attacks can impact blockchain networks as social, productive technologies. However, because Ethereum is decentralised, it rapidly recovered evidence of the strength of blockchain technologies to isolate and denounce service attacks that do not inhibit the impacts of DDoS.

2. Solana Network

The Soleana blockchain was subjected to one of the largest examples of denial of service attacks in 2021, due to the substantial number of artificial transaction processing originating from bots which, in general ICO transactions, pure transaction flood attacks are the safest. Notwithstanding the overwhelming transaction processing, Solana quickly recovered, due to its decentralised architecture, emphasising that blockchains can withstand extreme traffic volume while maintaining service availability. Solana subsequently modified its security protocols after this experience indicating that blockchain value proposition and technology contributes to adaptation and change to new attacks.

A simple comparison between Traditional methods and Blockchain-Based Solutions:-

Feature	Traditional Methods	Blockchain-Based Solution
Scalability	Limited; can become overwhelmed	High; off-chain transactions reduce load
Cost Efficiency	High operational costs	Lower transaction fees via Lightning Network
Identity Management	Centralised; prone to breaches	Decentralised; enhanced security
Response Speed	Slower; manual intervention often needed	Automated responses via smart contracts
Data Integrity	Vulnerable to tampering	Immutable ledger; high integrity
Privacy	Limited; easily traceable	Enhanced privacy with Schnorr signatures

Conclusion :- The implementation of blockchain technology is a viable solution to reduce the risks of DDoS attacks across the telecommunications sector. Its qualities of decentralisation, immutable ledgers, automated smart contracts, and economic deterrent properties can improve security and resiliency against attacks. Although it faces certain challenges such as transaction flooding attack risks, resource usage, integration issues, and regulatory challenges must be addressed before the full potential of blockchain technology is available to protect the country’s critical infrastructure. Case studies involving Ethereum, Solana and Arbitrum illustrate the adaptability of blockchain technology can lead to new advances in future telecommunications cybersecurity developments.

Discussion :-

Significance of Results :-

1. Threat Landscape is Increasing :-

The 30% year-on-year increase in cyberattacks (to 420 million in the year) on critical infrastructure globally indicates a growing threat to national assets, including telecommunications.

The spike in year-on-year DDoS attacks by 47%, particularly against government services, illustrates the geopolitical nature of the threat and its ability to negatively affect critical national infrastructure.

2. Attacks are Becoming More Sophisticated :-

The fivefold increase in devices involved in DDoS attacks (from 4,000 to 20,000) represents a considerable increase in attack capabilities, which will create more problems for defence mechanisms that have been previously effective.

The doubling of DDoS attacks in 2023 and the increase in attacks lasting more than an hour also demonstrate the ongoing and increasing persistence of attacks.

3. Vulnerability of Telecommunications

The fivefold increase in DDoS attacks specifically against telecommunications shows its value to, and vulnerability within, critical infrastructure.

Attacks on Indian airports and hospitals in April 2023 illustrate that critical infrastructure is intrinsically tied together and that disruptions to telecommunication can have cascading impacts.

4. Economic Impact

With an average loss of $1.188 million per DDoS attack, and losses of up to $1 million an hour for large organisations, the economic impact on the sector and related industries must be substantial.

5. Problems with traditional security measure

The analysis of traditional DDoS mitigation techniques (rate limiting, IP filtering, blackholing, etc.) reveals issues with more sophisticated attack capabilities.

The human factor is a substantial vulnerability to DDoS attacks, highlighted by a major Indian telco phishing attack on 5 million customers that resulted in significant impacts.

6. Value of Blockchain Solutions :-

Because of the decentralised nature of blockchain technology, blockchain programs displayed an ability to return to service quickly after attacks, including Ethereum and Solana.

The promise of smart contracts and economic deterrents through proof systems present the desire to automate some type of defence or to prevent any attacks.

Questions Addressed :-

1. Why is telecommunication infrastructure significant to Nation’s economy and national security?

Although the results do not provide this directly for India in particular, we can derive evidence of its importance from the global trends:As in many nations, telecom infrastructure is a key part of national infrastructure, and essential for communication, commerce, and governance.With attacks aimed at telecom sectors globally seeing a 5 times increase in DDoS attacks, it is apparent that it is indeed a critical sector.The DDoS attack on Indian airports and other critical sectors (health) in April of 2023 demonstrates how the telecom sector is interconnected to other critical sectors.

2. What types of attacks present the greatest threat of cybersecurity to India's telecommunication infrastructure during geopolitical conflict?

With respect to the question:DDoS attacks, for example, are a major threat, with 47% annual increase globally.The average DDoS attack, in terms of duration, is also increasing, with many attacks now exceeding 20 minutes in duration, as well as increasing incidents that exceed 1 hour to 50% of an attack.Social engineering attacks and especially phishing attacks are also significant (e.g., the major Indian telco incident that affected 5 million customers).

3. How can Pakistan and China convert attacks to India's telecommunication infrastructure during geopolitical tension, in a detrimental way?

The results do not mention Pakistan or China attacking India directly,butThe results do indicate China is one of the leading cyberattackers throughout the globe.In light of geopolitical tension, it is reasonable to infer that the aforementioned countries may immediately affect India's telecom infrastructure to severely degrade communication, spread disinformation, and/or collect intelligence.

4. How could DDoS attacks serve as a weapon during geopolitical tension?

The research indicates:DDoS attacks are exceptionally disruptive, and can cost $1.188 million on average per attack.DDoS attacks may focus on cripple critical services. (see, attacks on Indian airports, and health institutions).It is also noted that attacks may increase up to 1 Tbps.This large attacks would lead to huge swaths of unintended services down just due to DDoS.

5. To what degree does telecommunications interdependence with other critical infrastructures amplify the DDoS risk of geopolitical conflict exploring other critical services (e.g. energy, finance)?

The results suggest significant interdependence: The April 2023 attacks on Indian airports and healthcare institutions demonstrate how telecom disruptions can affect multiple sectors.The targeting of government services (34% of all DDoS attacks) indicates the potential for cascading effects across various critical infrastructure sectors.

6. Does a decentralised blockchain system offer better DDoS attack aversion over centralised infrastructure vulnerabilities?

The results indicate potential advantages:Blockchain's decentralised nature distributes data across many nodes, making it more resilient to attacks.Case studies of Ethereum and Solana networks show rapid recovery from DDoS attacks, demonstrating blockchain's resilience.

7. Can blockchain technology effectively enhance the resilience of India's telecommunications infrastructure against DDoS attacks?

The results suggest potential effectiveness , Blockchain's decentralised nature could provide better resilience against DDoS attacks.Smart contracts could enable automated defence mechanisms.Economic deterrents through proof systems could make attacks more costly and less feasible.

8. What are the advantages of using blockchain technology to secure India's telecommunication infrastructure?

The results highlight several advantages:Improved security through immutable ledgers, making it difficult for attackers to alter records.Enhanced resilience due to decentralisation, eliminating single points of failure.Automated defence mechanisms through smart contracts.Economic deterrents that make attacks more costly to execute.

9. What barriers and limitations exist in implementing blockchain technology in the telecom industry?

The results highlight several challenges:Transaction flooding vulnerability: Blockchain networks can still be susceptible to transaction flooding attacks.Resource intensity: Implementing blockchain solutions requires considerable computational resources.Complexity of integration: Integrating blockchain into existing telecom infrastructure can be complex.Regulatory and compliance issues: The use of blockchain in critical infrastructure raises regulatory concerns, particularly regarding data privacy and security compliance.

Suggestions for Practical Applications :-

A Comprehensive Solution to Protect National Critical Infrastructure in the Telecommunications Sector Using Blockchain Technologies

Executive Summary

The telecommunications sector plays a crucial role in national security as well as the stability of the economy. This is particularly so for government entities, such as the Department of Defense, and private telecommunications companies. Cyber threats, such as, Denial of Service and Distributed Denial of Service attacks, have become much more sophisticated in both methodology and implementation. Utilising technology such as private blockchains, Hyperledger Fabric, the Lightning Network, and Schnorr signatures can ultimately increase the security and resiliency of the infrastructure. This paper describes how to leverage that technology, how to utilise it economically, and the advantages and disadvantages of each from a governmental and private sector perspective.

Government Agencies (Defence) Solution :-

1. Private Blockchain with Hyperledger Fabric. Government agencies can implement a private blockchain with Hyperledger Fabric to provide a secure, permissioned network to manage sensitive telecommunications data. The Certificate Authority (CA) of Hyperledger Fabric can manage identities, so only authorised persons can access critical systems. All transactions are immutably recorded, meaning any transactions can not be modified and provide a non-tamper audit trail critical for national security. Threats, anomalies, or attacks can be automatically tracked or responded to by using smart contracts, meaning if a DDoS attack is detected it can rapidly mitigate the imminent threat.

Pros: Decentralised identity management will provide enhanced security for data. The immutability will improve integrity and provide transparency on data access. The automated response to potential threats can provide rapid reaction times.

Limitations: The implementation and ongoing operation would be costly and complex, inclusive of the use of specialised personnel. The ongoing user or operational costs could be considerable, e.g., infrastructure plus training.

2.Lightning Network for Scalability :-

The lightning network can be implemented to allow rapid and low-cost transactions when there is high demand traffic. The off-chain transaction capability will allow a large volume of transactions to be processed without overloading the underlying blockchain. This is valuable especially if there is a DDoS attack or large traffic. The government agency can prioritise level of service to real-time payment channels and ensure they are obtaining the reliability and bandwidth they require to facilitate critical communications .

Pros: This will allow government agencies to rapidly complete large volumes of high-frequency transactions. The payment solution set-up costs would now be reduced operationally.

Limitations: Potentially, centralization or monopolisation issues can arise if larger and precedent firms exert control, assumption or a 'host' network model of effect. Distributed routing protocols can create new concerns about security vulnerabilities.

3.Schnorr Signatures for Enhanced Security Authentication :-

Schnorr signatures can be implemented to provide secure identity management and transactions verifications. Schnorr signature sets are compact in size, therefore use reduced memory, speculative bandwidth and higher transaction volume. Schnorr signatures allow for multi-signature approvals to enable collaboration and add further security to transactions.

Pros: Schnorr signatures allow for easy usage while having enhanced security against forgery or tampering. Processing transactions will be more efficient with Schnorr Signature approvals and confirmations.

Limitations: Careful implementation must be conducted so that a nonce is not reused as nonces are exploited allowing a private key to be compromised. Complexity in integrating with existing systems may pose challenges.

2.Solutions for private telecommunications firms :-

1. Private blockchain utilising Hyperledger Fabric :-

How will it be implemented? Private telecommunications firms can adopt Hyperledger Fabric to increase operational efficiency, as well as security.

Decentralised operations: Using a private blockchain means that telecommunications firms manage customer data and avoid some of the risks associated with data breaches.

Smart contracts for billing: By utilising smart contracts vendors can greatly minimise human error in billing processes, and better productivity.

Pros:

Increased transparency and trust with customers.

Increased security through decentralised identity management.

Cons:

High cost of implementation and training.

Complexity of managing a 'permissioned' network.

2. Lightning network for cost effectiveness :-

How will it be implemented? Among other things, telecommunications companies can utilise the Lightning Network from Bitcoin to manage microtransactions and improve service delivery.

Direct transaction system: Customers are able to simply pay for services and utilisation of direct payments means that it is not necessary for vendors to use an intermediary to process payments and thus drives down on-off operational costs.

Scalable infrastructure: The Lightning Network is a distributed payment structure, ensuring capabilities to accommodate growing transaction volume, and service delivery without degrading consumer service.

Pros:

Reduced costs of operation, and other economies of scale in improving the customer experience.

Supports future scalability.

Cons:

Potential to lead to centralization.

Added risk of insecurity associated with 'off-chain' transaction verification.

3. Schnorr Signatures as a tool to increase transaction security

How will it be implemented? The Schnorr signature is capable of supporting various financial transaction needs of telecommunications firms, as well as transactional identity verification.

More efficient verification: Schnorr signatures allow for more efficient verification of either simple or large complicated contract transactions.

Maximising investments: Schnorr signatures will allow for better workflow regarding multi-signature processes; and thus help to enhance security and integrity for example, with joint transactions.

Pros:

Better security and potential to minimise forgery.

Worker productivity.

Better scalability of information and identity verification process.

Cons:

Some complexity of implementation requires experienced employees.

Case specific factors to manage or supervise signature validation.

Conclusion of discussion :-

The combination of Hyperledger Fabric, private blockchain technology, Schnorr signatures, and the Lightning Network represents a comforting structure for partially securing national critical infrastructure in the context of the telecommunications industry. Government organisations and private telecom providers may experience improved security, efficiency, and savings through these technologies; however, they must navigate challenges related to complexity of implementation, and lack of skilled personnel, in the implementation of these technologies. By purposefully addressing limitations, stakeholders should be able to develop a robust telecommunications infrastructure that withstands the changing landscape of cybercrime, hacking, and the threat of cyber-attacks.

Conclusion : -

There is a growing concern about the impact of Distributed Denial of Service (DDoS) attacks on national critical infrastructure within India's telecommunications sector. With more than 420 million reports of cyberattacks (trends), including severe ones on Indian infrastructure, it is evident that updated cybersecurity approaches must be adopted. Although traditional defences are necessary, they may not mitigate DDoS or critical infrastructure exposures to threat actors, especially with growing risks for advanced threats and the rapid evolution of threat actors. The study observes a significant acceleration of attacks, frequency and seriousness of attacks, with the availability of geopolitical tensions, evolving technologies, and improvisation in operational capabilities. Even with operational improvements, these practices have diminishing consideration by previous operationalizations.

The study indicates that there is significant potential for cybersecurity resilience benefit attributes from the advancement of blockchain technology. The benefit of a decentralised, immutable ledger (i.e., blockchain), smart contracts, and automated defence mechanisms bring real value (versus Operationalizing, etc) to tackle DDoS and secure infrastructure. However, limitations of transaction flooding mechanisms, significant resource, and regulatory attribute/settlement would have to be resolved. These were highlighted by the case transportation studies within the Ethereum and Solana networks. These studies exemplified a general use of blockchain to ensure operational integrity during immediate availability of DDoS attacks.

Overall, the study is anticipated to support the design of intuitive technology blockchain development to augment engineering frameworks. Future DApps developments would have to be considered as transaction settlements for credible integrations. Exploring blockchain infrastructures with applicable knowledge systems for transaction architectures would be an evolution to enhance resiliency. A more engaged approach would include investigating regulatory practices and tactics to repel or avoid advanced threat authoring.

However , to achieve the full potential of blockchain, obstacles including transaction volume issues, resource intensity problems, and regulatory compliance issues must be overcome. In summary, this study highlights the importance of a proactive and integrated approach to cybersecurity in telecommunications, and it recommends that blockchain technology be prepared and aligned as a solution for protecting national critical infrastructure against cyber attacks.

Acknowledgement :-

Professor's and teaching staff at Ramnarain Ruia Autonomous College .

References :-

1. Websites :-

1.https://www.cert-in.org.in/

2.https://nciipc.gov.in/

3.https://www.nist.gov/cyberframework

4.https://www.nsa.gov/

5.https://www.cisa.gov/

6.https://www.meity.gov.in/

7.https://www.statista.com/

2.Articles :-

1.https://www.hindustantimes.com/ht-insight/future-tech/the-new-cyberspace-doctrine-s-impact-on-indias-security-101720843641057.html

2.https://www.drishtiias.com/daily-updates/daily-news-editorials/india-s-cybersecurity-challenge-threats-and-strategies

3.https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html

4.https://www.cisco.com/c/en/us/products/collateral/security/ddos-5steps-protect-organization-so.html

5.https://www.cloudflare.com/en-in/learning/ddos/how-to-prevent-ddos-attacks/

6.https://www.telecomreview.com/articles/reports-and-coverage/4865-telecommunication-security-ddos-attacks

7.https://socradar.io/global-ddos-attack-landscape-insights-from-q1-2024/

8.https://www.comparitech.com/blog/information-security/ddos-statistics-facts/

9.https://digitalisationworld.com/news/66951/average-ddos-attack-cost-businesses-325000

10.https://enterprisetalk.com/featured/businesses-need-to-know-about-hyperledger-fabric-in-blockchain/

11.https://www.radware.com/blog/security/2013/05/how-much-can-a-ddos-attack-cost-your-business/

12.https://industrialcyber.co/critical-infrastructure/critical-infrastructure-faces-30-percent-surge-in-cyber-attacks-knowbe4-report-highlights/#:~:text=%E2%80%9CBetween%20January%202023%20and%20January,a%2030%25%20increase%20from%202022.

13.https://www.cfr.org/cyber-operations/targeting-ukrainian-telecommunication-companys-internet-service

14.https://kratikal.com/blog/how-recent-cyber-attack-took-down-entire-telcom-industry-in-ukraine/

15.https://stormwall.network/ddos-report-stormwall-q1-2024

16.https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023

2. Reports :-

1.Vodafone. (2023). Annual Cybersecurity Report.

2.Telefónica. (2023). Digital Security Insights.

3.Orange. (2022). Business Services Security Update.

4.AT&T. (2023). Cybersecurity Effectiveness Report.

5.Deutsche Telekom. (2023). Security Operations Center Annual Review.

6.GSMA. (2023). Telecommunication Security Landscape.

7.BT Group. (2022). Zero Trust Security Implementation Case Study.

8.ENISA. (2023). 5G Threat Landscape Report.

9.The Economic Times. (2022). "Major Data Breach at Indian Telecom Giant".

10.UK Department for Digital, Culture, Media & Sport. (2023). Telecom Security Report.

11.European Commission. (2023). 5G Infrastructure Security Assessment.

12.Cybersecurity Insiders. (2022). "Massive IoT Botnet Disrupts European Telecoms".

13.NIST. (2023). PostQuantum Cryptography Readiness Survey.

14.European Data Protection Board. (2023). Annual Report on GDPR Enforcement.

15. (ISC)². (2023). Cybersecurity Workforce Study: Telecom Sector Analysis.

16.https://blog.knowbe4.com/

3. Research Papers :-

1.in-risk-Building-cyber-security-into-critical-infrastructure-noexp(deltio).pdf

2.2019–2023 in Review: Projecting DDoS Threats With ARIMA and ETS Forecasting Techniques"

3.V. R. Fedik and H. V. Denysenko, "Theoretical and Methodological Approaches to Cybersecurity Risk Management at Critical Infrastructure Facilities: Responding to 4.Cyber Incidents and Crisis Situations Management," Information and Law, vol. 1, no. 48, pp. 194–202, 2024

5.Olufunsho I. Falowo and Jacques Bou Abdo, "2019–2023 in Review: Projecting DDoS Threats With ARIMA and ETS Forecasting Techniques,"

6.CERT-In, “INDIA RANSOMWARE REPORT,” 2022.

7.CSIRT-Fin, CERT-In, and Mastercard, "API Security: Threats, Best Practices, Challenges, and Way forward using AI," Aug. 2023

8.P. Kivimaa, "Graded Security Expert System," in Proceedings of the 11th International Conference on Information Security and Cryptology (ICISC 2008), Seoul, Korea, December 3-5, 2008, pp. 372-387.

9.B. Ojo, J. C. Ogborigbo, and M. O. Okafor, "Innovative Solutions for Critical Infrastructure Resilience Against Cyber-Physical Attacks," World Journal of Advanced Research and Reviews, vol. 22, no. 03, pp. 1651–1674, 2024. doi: 10.30574/wjarr.2024.22.3.1921

10.R. Naidoo and C. Jacobs, "Cyber Warfare and Cyber Terrorism Threats Targeting Critical Infrastructure: A HCPS-based Threat Modelling Intelligence Framework," in Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019), Prague, Czech Republic, February 19-21, 2019, pp. 443-450.

11.I. Cesarec, "Beyond Physical Threats: Cyber-attacks on Critical Infrastructure as a Challenge of Changing Security Environment – Overview of Cyber-security Legislation and implementation in SEE Countries," Ann. Disaster Risk Sci., vol. 3, no. 1, 2020.

12.U.S. Government Accountability Office, “Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure,” GAO-23-106441, 2023.

13.M. Y. Lin and J. Nunn-Price, "Building cyber security into critical infrastructure: Protecting industrial control systems in," Deloitte, 2020.