NATIONAL LAW INSTITUTE UNIVERSITY BHOPAL

Master of Cyber Law and Information Security

BATCH 2024-26

CRYPTOGRAPHY AND NETWORK SECURITY

Project Assignment On

"NETWORK SECURITY FOR PUBLIC SECTOR ORGANISATIONS"

Under the Supervision of

Dr. AMITESH SINGH RAJPUT

Assistant professor

Computer science

Submitted By

MEENAKSHI PUNDHIR
2024MCLIS27

I semester

ACKNOWLEDGEMENT

I want to take a moment to express my heartfelt gratitude to everyone who supported me throughout the journey of my project on "*Network Security for Public Sector Organisations*."

First and foremost, I am deeply thankful to Dr. S.Suryaprakash, our Vice Chancellor. His unwavering support and motivation were instrumental in helping me navigate the challenges and strive for excellence in my work.

I am also sincerely grateful to Mr. Vivek Bakshi, our Registrar. His guidance and readiness to assist ensured that I had everything I needed to move forward with confidence.

A special thanks goes to my professor, Dr. Amitesh Singh Rajput. His mentorship was invaluable, providing me with advice and insights that kept me focused and helped refine my research.

Lastly, I would like to acknowledge the Library staff of National Law Institute University, Bhopal. Their assistance in accessing essential resources played a crucial role in the success of my project.

I truly appreciate the support and encouragement from everyone involved, and I am incredibly grateful for the time and effort each of you dedicated to helping me succeed.

Thank you all so much.

Meenakshi Pundhir
Roll No. 2024MCLIS27
I Semester

Contents

ABSTRACT

Public sector organisations in India are increasingly targeted by cyberattacks due to their role in managing critical national infrastructure and sensitive citizen data. This research project aims to explore the network security challenges faced by four key public sectors: financial services, telecommunications, healthcare, and the Aadhaar system. Through a comprehensive analysis of cyberattacks specific to these sectors, including incidents of data breaches and ransomware, this study will identify prevalent vulnerabilities and threat vectors. The research will also investigate the underlying factors contributing to these security gaps, such as technological inadequacies, regulatory shortcomings, and human error. Based on this analysis, the project will propose solutions designed to enhance the resilience of public sector networks. These recommendations will encompass a range of strategies. The ultimate objective is to provide actionable insights that can be implemented by the public sector organisations to safeguard against future cyber threats.

Keywords: Network Security, Cybersecurity, Public Sector, Ransomware, Financial Services, Telecommunications, Healthcare, Aadhaar System.

ABBREVIATIONS

1. **VPN** - Virtual Private Network
2. **IDS** - Intrusion Detection System
3. **IPS** - Intrusion Prevention System
4. **NDR** - Network Detection and Response
5. **XDR** - Extended Detection and Response
6. **DNS** - Domain Name System
7. **DDoS** - Distributed Denial of Service
8. **DoS** - Denial of Service
9. **SIEM** - Security Information and Event Management
10. **SLAs** - Service Level Agreements
11. **MAC** - Mandatory Access Control
12. **XSS** - Cross-Site Scripting
13. **SWIFT** - Society for Worldwide Interbank Financial Telecommunication
14. **CBS** - Core Banking System
15. **EHR** - Electronic Health Records
16. **PII** - Personally Identifiable Information
17. **PHI** - Protected Health Information
18. **MITM** - Man-in-the-Middle
19. **UIDAI** - Unique Identification Authority of India
20. **SQL** - Structured Query Language
21. **HTTP** - Hypertext Transfer Protocol
22. **HSTS** - HTTP Strict Transport Security
23. **CAPTCHA** - Completely Automated Public Turing test to tell Computers and Humans Apart.
24. **IP**- Internet Protocol
25. **MFA**- Multi-factor Authentication

CHAPTER 1: INTRODUCTION

In an era where our lives are increasingly intertwined with digital systems, the security of public sector networks has never been more critical. Imagine a scenario where a hospital's network is compromised, putting patient data at risk, or a breach in the Aadhaar system exposes millions of identities. They are not just abstract threats- they are the real possibilities that could disrupt essential services and erode public trust.

In the realm of cybersecurity network security plays a role in safeguarding computer networks and systems, against both internal and external cyber threats and attacks. The main goals of network security are to stop access to network resources effectively and to identify and halt cyber attacks and security breaches in action while ensuring that authorized users can securely access the required network resources promptly as needed.

While both public and private sector are subjected to network security vulnerabilities, the public sector faces a much bigger challenge to cybersecurity, both at the international and national level.

In case of India, network security for public sector organisations is of particular importance given the government's push to digitise a wide array of services under initiatives like Digital India. According to reports from the *Indian Computer Emergency Response Team (CERT-In)*, the organization responsible for monitoring and tracking cybersecurity incidents in India, there were 70798, 85797, 54314, 48285, 192439, and 112474 cybersecurity incidents involving government organizations or systems in 2018, 2019, 2020, 2021, 2022, and 2023, respectively.[1] We can clearly see the year by year growth in cybersecurity incidents and it is alarming.

The purpose of this study is to examine the particular network security vulnerabilities present in public sector organizations across four key domains: finance, administration, healthcare, and telecommunications. Through an analysis of secondary data sources, including published reports, academic studies, and established security protocols, the research will pinpoint prevalent weaknesses and industry-specific security challenges. The ultimate goal is to deliver a thorough assessment of the current security environment and propose actionable strategies for bolstering network protection within these vital sectors.

[1] 'Cyber Security: Over 1 Lakh Cyber Security Incidents in Govt Organisations This Year - The Economic Times' <https://economictimes.indiatimes.com/tech/technology/over-1-lakh-cyber-security-incidents-in-govt-organisations-this-year/articleshow/102362589.cms?from=mdr> accessed 1 September 2024.

1.1 REVIEW OF LITERATURE

1. ***Suman Acharya and others, "Impact of cyberattacks on banking institutions in India: a study of safety mechanisms and preventive measures" (2020):*** The literature on cybercrime's impact on banking institutions paints a grim picture, with numerous Indian banks falling victim to massive malware attacks. The literature finds that major cybercrimes in the Indian banking sector stem from phishing, identity theft, and malware, necessitating regular system audits and vigilant monitoring of ATM/POS connectivity. It suggests that public sector banks should enhance security through public-private partnerships and increased budgets for data protection.
2. ***Abdul Salam Mohammed, "Privacy and security risks with Aadhaar card: study of media discourses on reporting various third party data breaches" (2022)":*** The literature highlights the significant role of media in reporting third-party breaches of Aadhar cards, focusing on critical discourse analysis. It categorizes breaches into data leakages, privacy issues, security breaches, and data protection measures. Intentional threats, such as improper encryption, are more prevalent than unintentional ones. The study underscores the need for robust actions by UIDAI to safeguard the Aadhar ecosystem from these persistent threats. The study's findings are limited due to the small number of articles on third-party data breaches and the focus on specific security and privacy issues, making generalization difficult.
3. ***Rithik V Gopal, "Aadhaar Data Breach — How Sensitive Data Of 1.3 billion Indians Was Compromised" (2022)***: The article on the Aadhaar data breach investigates how the exposure of personal data affected 1.3 billion individuals due to systemic vulnerabilities. As per the article, a software patch allowed users to bypass important security measures, like biometric authentication for enrolment operators, enabling the creation of unauthorized Aadhaar numbers. The article also emphasizes the need for enhanced security measures and regulatory oversight to protect sensitive information.
4. ***Dharm Patel, "Case study: 2018 Pune's Cosmos Bank Cyberattack" (2023):*** This article on review of the 2018 Cosmos Bank cyberattack explains how a spear phishing attack likely compromised the bank's ATM infrastructure via malware, severing the connection between the ATM switch and the Core Banking System (CBS).The attackers then installed a proxy switch, gaining control over the ATM operations. The author also connects the incident to wider cybersecurity trends, stressing the importance

of stronger security measures and continuous monitoring to protect financial institutions from future attacks.

5. ***Dr. Parvathi Balaji and others, "Cyber Attack - Envenom in Indian Healthcare – A Review***": Cybersecurity has become a major concern for healthcare organizations, especially since the pandemic. Electronic health records, while beneficial for patient care, have also become targets for cybercriminals. Phishing attacks are on the rise, and it's clear that healthcare providers need to prioritize cybersecurity education and implement stronger protective measures to safeguard patient data.

1.2 STATEMENT OF PROBLEM

Public sector organizations in finance, health, administration, and telecom are facing an increasing wave of cyberattacks, even with security measures in place. Financial sector struggles with a variety of cybersecurity threats like DDoS and phishing, health sector handles sensitive health information which often falls prey to cyber attacks like ransomware, important aspect of administration is Aadhaar system which suffers from threats to privacy while telecom sector is a bridge to all these sectors which suffers from its own problems. This study aims to uncover these gaps and offer customized solutions to strengthen defenses against these growing cyber threats.

1.3 HYPOTHESIS

Government agencies in the financial, health, administrative, and telecommunication sectors are increasingly vulnerable to cyber threats due to inadequacies in existing security measures. If these sector-specific vulnerabilities are identified and addressed with tailored strategies, the resilience of government networks against evolving cyber threats can be significantly strengthened.

1.4 RESEARCH QUESTION

1. What are the most common types of cyber threats that imperil the network security of Public Sector Organisations in India?
2. What are the loopholes in network security framework of critical infrastructure of public sector organisations in India?
3. Are the current network security practices sufficient to address the specific challenges faced by these sectors?

4. What can be the best practices and solutions that can be applied to enhance the network security of the critical sectors?

1.5 RESEARCH OBJECTIVES

1. To understand the most prevalent kinds of cyberattacks that threaten the network security of public sector organisations in India.
2. To explore various network security vulnerabilities in the critical sectors like finance, health, telecommunication and Aadhaar system in India.
3. To critically examine the current network security practices followed by India Public Sector Organisations.
4. To identify the best practices and innovative solutions that can be tailored to meet the network security needs of Indian Public Sector Organisations.

1.6 SCOPE AND LIMITATION

This research aims to understand the kinds of cyber threats that critical Indian public sector organisations faces with a special focus on health, telecommunication, financial and Aadhar system. The primary focus is to identify the gaps in network security practices currently followed by these organisations and suggest tailored sector specific solutions to address the same.

1.7 RESEARCH METHODOLOGY

The researcher has chosen doctrinal method of research to investigate the topic of " Network Security for Public Sector Organisations."

CHAPTER 2: ANALYSIS AND DISCUSSION

Network security shields the network and data from breaches, invasions, and other dangers. This is a broad, all-encompassing phrase that covers software and hardware solutions, as well as procedures, guidelines, and setups for network usage, accessibility, and general threat protection. Network security includes firewalls, VPN encryption, application security, network analytics, access control, virus and antivirus software, and other network-related security measures (such as endpoint, web, and wireless).

Network security is essential for safeguarding client information and data, maintaining the security of shared data, guaranteeing robust network performance and access, and defending against online attacks. A carefully planned network security solution lowers overhead costs and protects businesses against significant losses resulting from data breaches and other security incidents.[2]

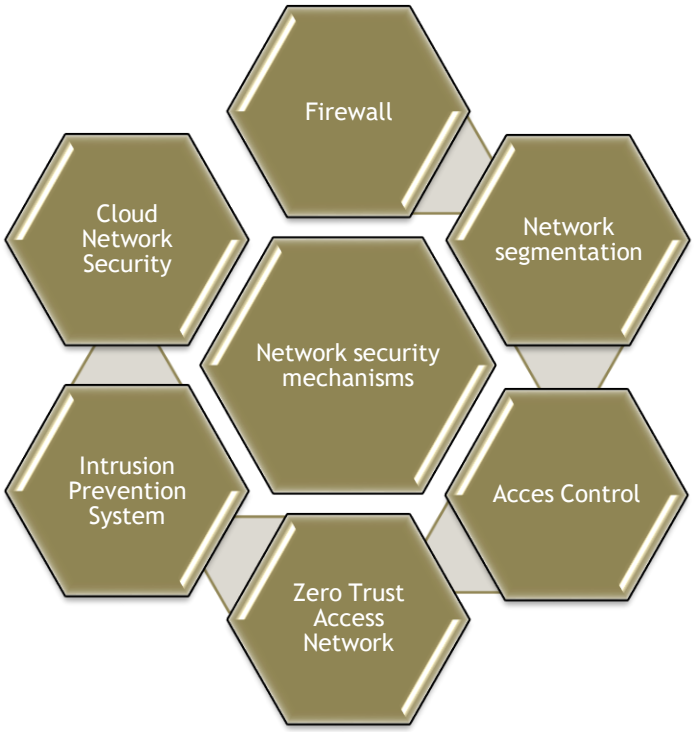

FIGURE 1: Network Security Mechanisms

[2] 'What Is Network Security? The Different Types of Protections - Check Point Software' <https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/> accessed 2 September 2024.

2.1 NETWORK SECURITY PRACTICES FOLLOWED BY INDIAN PUBLIC SECTOR ORGANISATIONS.

The *Indian Computer Emergency Response Team (CERT-in)* is empowered under Information Technology Act, 2000, to issue cybersecurity guidelines. These guidelines are mandatory for all government entities, including ministries, departments, public sector enterprises, and other agencies. CERT-in expects these entities to follow the guidelines to ensure robust cybersecurity practices across the public sector.

Following guidelines are advised to be followed by Indian Public Sector Organisations to enhance network security:

To enhance network security, several key strategies should be implemented. Begin by deploying tools like IDS, IPS, NDR, XDR, and firewalls to monitor and mitigate threats at the network perimeter. Next, secure both external and internal networks with NextGen firewalls in High Availability (HA) mode. Strengthen DNS security by using internal servers to block malicious requests and limit access to external DNS services. All internet traffic should be routed through proxy servers to ensure safety. Device logging must be enabled and integrated with a SIEM system, with logs retained for at least 180 days. DDoS protection measures, with clearly defined SLAs, are crucial for maintaining availability. It is essential to disable insecure protocols and prioritize secure ones such as SSH and IPsec. For remote access, VPNs should be secured with multi-factor authentication (MFA) and monitored regularly. Implement MAC address binding with manual IP configuration for added security, and always change default credentials and settings during initial installation to prevent unauthorized access.[3]

2.2 SECTOR-WISE ANALYSIS OF NETWORK SECURITY BREACHES IN INDIA'S CRITICAL SECTORS.

1. FINANCIAL SECTOR: From January to October 2023, India's banking sector experienced more than ***13 lakh*** cyberattacks, averaging about 4,400 daily, according to *the Reserve Bank of India*[4]. The primary attack methods included Denial of Service (DoS), web application attacks, and payment card skimming, accounting for over 88% of the incidents. Cybercriminals employ various tactics such as phishing to steal credentials, identity theft using personal data, and

[3] Bhupendra Singh Awasya, 'Guidelines on Information Security Practices for Government Entities'.
[4] '13 Lakh Cyber Attacks Hit Indian Banks in 10 Months; Who Is behind Them? - India Today' <https://www.indiatoday.in/diu/story/cyber-attacks-hit-indian-banks-rbi-report-swift-network-2481951-2023-12-29> accessed 2 September 2024.

viruses or Trojans often spread via spam emails. Vishing manipulates individuals through phone calls, while Cross-Site Scripting (XSS) targets web application vulnerabilities. Insider threats and botnets also pose significant risks, and ransomware attacks lock data until a ransom is paid. These breaches highlight critical vulnerabilities and underscore the urgent need for improved cybersecurity measures.

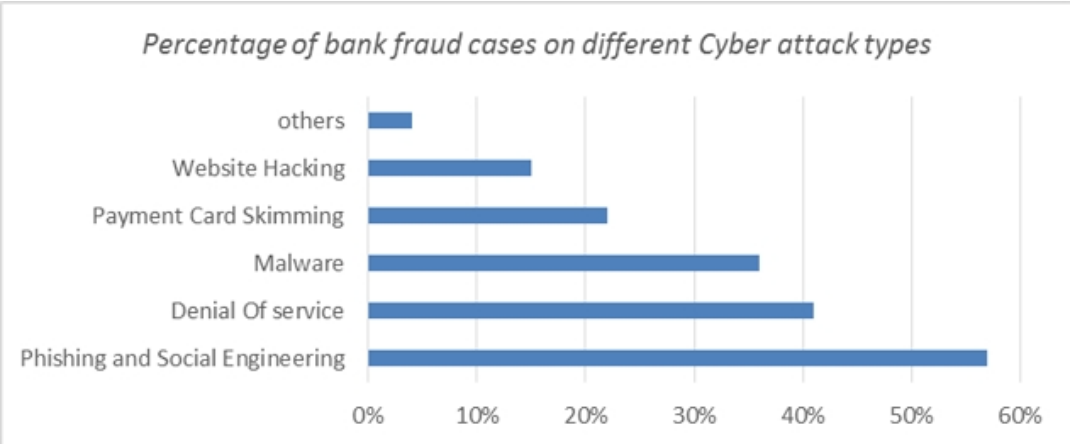

FIGURE 2: Banks and cyber attacks.[5]

CASE STUDY OF COSMOS COOPERATIVE BANK PUNE.

In August 2018 and 2019, Cosmos Cooperative Bank in Pune was hit by major cyber-attacks targeting its ATM and SWIFT systems. Hackers exploited these systems to make unauthorized transactions, stealing over Rs. 84 crore. The bank acted quickly to recover Rs. 8 crore and worked hard to get everything back on track, but the attacks caused significant disruptions and financial losses. Customers grew worried, leading to premature withdrawals and lost card commission revenue.

The Cosmos Cooperative Bank's ATM infrastructure was likely compromised by *malware* delivered through a spear phishing attack. This malware disrupted the connection between the bank's Core Banking System (CBS) and its ATMs, allowing hackers to take control of the ATMs and make unauthorized cash withdrawals. The attackers installed a proxy switch to manipulate account balances and facilitated global cash withdrawals by designated mules. Because the CBS was bypassed, these transactions went unrecorded. The preparation for this heist probably began months earlier, involving the theft of customer data and cloning of cards.

The attack on Cosmos Cooperative Bank showcases various network vulnerabilities that commonly exists in public sector banks. These include weak phishing defense and inefficient

[5] 'CyberSecurityConclaveAtVigyanBhavanDelhi_1 (1)'.

malware protection, security gaps in ATM and POS systems, inadequate network segmentation allowed the malware to disrupt the connection with core banking system. Improper monitoring led to failure to detect unauthorised transactions. Additionally, gaps in data protection contributed to the breach of customer information and credit card cloning.[6]

2.HEALTH SECTOR: Technology adoption has completely changed the healthcare industry. Patients are no longer required to keep track of paper records. Their lives have been considerably simplified by telemedicine, IoT devices, and electronic health records (EHR). However, it has led to the emergence of a new threat: sensitive patient data theft. According to a report by *Check Point Software Technologies Ltd.*, there were 6,935 attacks on average every week in the Indian healthcare sector, whereas there were 1,821 attacks on average per healthcare organization worldwide.[7] The multiple breaches highlight deficiencies in the digital infrastructure of the Indian healthcare industry. Attacks often exploit IT infrastructure weaknesses due to misconfigurations, such as with firewalls, and can overwhelm services through DDoS. Software bugs, including privilege escalation and MITM, and cryptographic attacks also pose risks. Ransomware specifically targets healthcare by encrypting data and demanding ransom. Additionally, exploiting human weaknesses to gain access to healthcare infrastructure is an increasing concern.[8]

CASE STUDY OF AIIMS RANSOMWARE ATTACK.

Cyber attacks are becoming a more frequent hazard to organizations worldwide, and the attack on the All Indian Institute of Medical Sciences (AIIMS) serves as a stark reminder of the importance of putting cyber security measures in place. The November 23,2022 attack on AIIMS disrupted critical operations and rendered crucial systems non-functional, impacting five servers and encrypting 1.3 terabytes of data. The Indian Computer Emergency Response Team (CERT-In) investigated the incident and discovered that inadequate network segmentation was the root cause.

A ransomware attack made the main server and application in charge of the outpatient department (OPD) services to inaccessible. By changing their extensions to the new ".bak9"

---

[6] 'Case Study: 2018 Pune's Cosmos Bank Cyber Attack | by DHARM PATEL | Medium' <https://medium.com/@20dcs071/case-study-2018-punes-cosmos-bank-cyber-attack-cafd221cac25> accessed 11 September 2024.

[7] 'India's Healthcare Sector Top Target of Cybercrimes: Report - India Today' <https://www.indiatoday.in/india/story/healthcare-sector-top-target-of-cybercrimes-hacking-aiims-icmr-2561733-2024-07-03> accessed 11 September 2024.

[8] Dr Parvathi Balaji and others, 'Cyber Attack - Envenom in Indian Healthcare – A Review' (2023) 4 International Journal of Research Publication and Reviews 1262.

file type, all system files in the home directory were encrypted during this attack, thereby encrypting the original system files. Wannacry, Mimikatz, and Trojan were the three ransomwares that had infected the targeted systems. The cyber attack happened because of lack of proper centralised monitoring, inapt system administration and a disorganised information and communication technology (ICT) network .The affected devices were interconnected, allowing access of the data from any of these connected devices. Alarmingly, there was no dedicated team overseeing or monitoring the access to these system.

3.AADHAAR SYTEM: Governments worldwide are shifting from paper-based systems to digital identities, aiming to create more efficient economies. India's Aadhaar is a prime example: a unique 12-digit number assigned to each citizen, managed by the UIDAI, that includes biometric data like iris scans and fingerprints. As of late 2021, over 1.3 billion Aadhaar numbers have been issued.

CASE STUDY OF AADHAAR DATA BREACH.

Between 2017 and early 2019, numerous Aadhaar data breaches exposed millions of personal records. Leaks included children's Aadhaar information, bank details, and sensitive health data, often due to misconfigured government and industry websites. Notably, by early 2018, faulty software and security lapses had made the entire Aadhaar database vulnerable. In early 2019, a misconfigured site exposed 6.7 million records, highlighting ongoing issues with data security and access control.

A critical security flaw was exposed when a software patch, available for just $35, allowed unauthorized individuals worldwide to create fake Aadhaar numbers. This patch bypassed essential security measures, such as biometric authentication and GPS location tracking, making it possible to spoof the system from anywhere. Additionally, the patch weakened the iris-recognition system, allowing easy impersonation. Meanwhile, over 70 subdomains on a Government of India website provided unregulated access to Aadhaar verification Application programming interface (APIs), enabling hackers to exploit this vulnerability and access sensitive personal data. These issues not only breached privacy but also violated the Aadhaar Act.[9]

[9] 'Aadhaar Data Breach — How Sensitive Data Of 1.3 Billion Indians Was Compromised | by Rithik V Gopal | The Deep Hub | Medium' <https://medium.com/thedeephub/aadhaar-data-breach-how-sensitive-data-of-1-3-billion-indians-was-compromised-cb01d0c2d7d3> accessed 11 September 2024.

4.TELECOMMUNICATIONS SECTOR: Cybersecurity is a major concern for the telecom industry, which handles massive amounts of sensitive personal and financial data. With telecom networks critical for everything from phone calls to online banking, any breach can have severe consequences. As per a research by *CheckPoint Research (CPR*), the sector has seen a staggering 51% increase in cyber-attacks, making it the third most vulnerable industry after government and finance.[10]

CASE STUDY OF BSNL DATA BREACH 2024.

India's telecom giant BSNL recently faced a serious data breach, with hackers stealing sensitive information about its customers. This breach has resulted in personal details like names, email addresses, billing information, and call records being sold on the dark web. The leaked data includes about 32,000 lines from a sample set, and the total number of exposed records could be around 2.9 million. Both BSNL fiber and landline users are affected. The breach was reported by a threat actor using the alias "Perell."

The data structure found on the dark web allegedly indicated a SQL injection attack, where malicious code is used to manipulate backend databases and access sensitive information that was meant to be hidden. SQL, or Structured Query Language, is used to interact with and manage databases.[11] SQL injection is a hacking technique where attackers use malicious SQL queries to access or manipulate sensitive data in a database through web applications. The SQL injection is a common method for breaches, as even well-known databases like MySQL have been compromised this way, exposing or altering valuable information.[12]

2.3 MEASURES TO ENHANCE THE NETWORK SECURITY OF CRITICAL INDIAN PUBLIC SECTOR ORGANISATIONS.

With over 80 Crore people interconnected and using the internet for varied purposes, India is quickly establishing itself as one of the most connected countries in the world. But the use of internet has also contributed to an increase in user harm and network security breaches.

---

[10] 'Telecom Turmoil – Cybersecurity Emerges as Top Priority amidst Rising Threats | Communications Today' <https://www.communicationstoday.co.in/telecom-turmoil-cybersecurity-emerges-as-top-priority-amidst-rising-threats/> accessed 11 September 2024.

[11] 'Threat Actor Breaches BSNL Server Database, Puts up Dataset on Dark Web | Company News - Business Standard' <https://www.business-standard.com/companies/news/threat-actor-breaches-bsnl-server-database-puts-up-dataset-on-dark-web-123122200310_1.html> accessed 11 September 2024.

[12] '(PDF) Review of SQL Injection : Problems and Prevention' <https://www.researchgate.net/publication/325940419_Review_of_SQL_Injection_Problems_and_Prevention> accessed 11 September 2024.

Cyberthreats that affect vital services and national. Public Sector organizations need to use best practices and robust network security measures to defend against these threats.

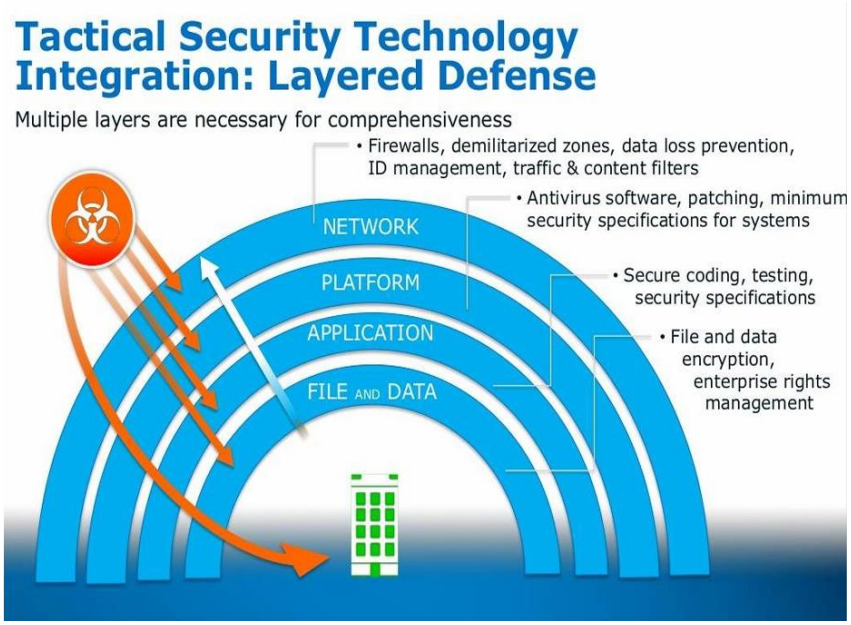

FIGURE 3:Layered defense for network security[13]

Following are some tailored sector specific solutions to address the loopholes in existing network security frameworks adopted by Indian Public Sector Organisations:

1.FINANCIAL SECTOR- The profound threats to banks posed by threat actors cannot be further overlooked. Banks need to develop a strong network security threat monitoring framework and also some "state-of-the-art" technologies to mitigate and manage risk. Following are some of the recommendation to ensure network security of financial sector:

1. **Giving primacy to Cybersecurity Assessment**- The banks should use a risk-based strategy to continuously assess threats, should prioritise cybersecurity maturity assessment and also, focus on combining financial crime reporting, fraud risk assessment, and cyber risk assessment
2. **Regulating access to third-party services**-The banks should prioritise alliance partners' and vendors' access to and availability of services and limit or restrict their access to core infrastructure of the respective bank and also, look into the possibilities of modifying contractual arrangements to keep an eye on third parties' access to banking infrastructure.

[13] 'CyberSecurityConclaveAtVigyanBhavanDelhi_1 (1)' (n 5).

3. **Implementing innovative technologies and solutions**- The banks should build multiple lines of defence at various levels within the security ecosystem and also adopt modern defence options, like Zero-trust architecture, Advanced endpoint security systems, augment cybersecurity with AI, DevSecOps

2.HEALTH SECTOR- Following are some of the recommendations to ensure network security in health sector-

1. **Vulnerability and Patch Management**: Regularly detect, evaluate, and address IT vulnerabilities using EDR tools and risk assessments. Conduct proactive vulnerability identification and penetration testing, as most exploits target known issues. Promptly remediate vulnerabilities to mitigate attack risks.
2. **Least Privilege and Multifactor Authentication**: Limit and monitor administrative privileges to reduce risks from compromised accounts. Enforce strong password policies and provide separate accounts for administrative and everyday tasks. Implement multifactor authentication for enhanced security across all accounts.
3. **Securing Medical Equipment:** Maintain an up-to-date inventory of medical devices and work with manufacturers for security updates. Enforce strict rules for personal device use and data encryption to protect connected medical equipment from cybersecurity threats.

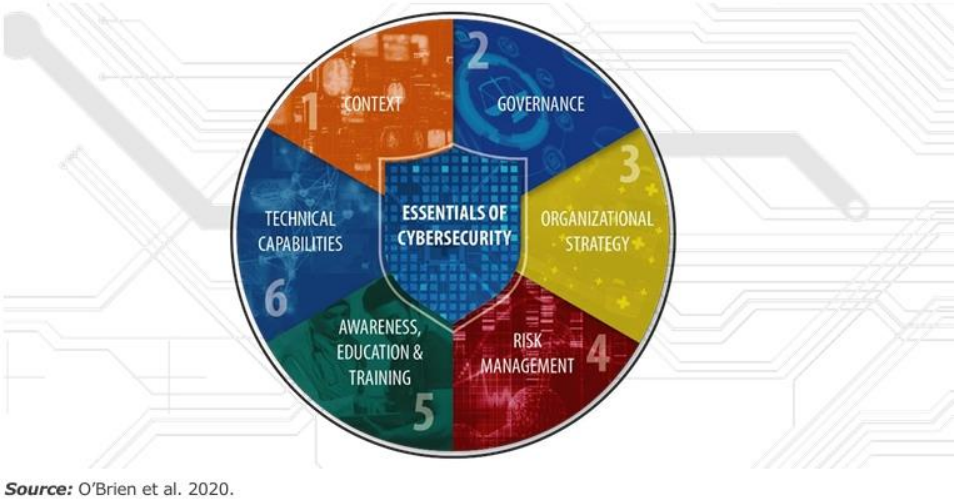

FIGURE 4: Essentials of cybersecurity for healthcare organisations (ECHO) framework.[14]

[14] 'P17507500a843000d099250f19a00b04019.Pdf' <https://documents1.worldbank.org/curated/en/099081723223525669/pdf/P17507500a843000d099250f19a00b04019.pdf> accessed 11 September 2024.

3.AADHAAR SYSTEM- Aadhaar, which initially was just a random number without personal details, now includes sensitive information like fingerprints, iris scans, and addresses. To protect this data from intruders, we recommend several preventive measures:

1. **Enforcing secure connections**: Activate HTTP Strict Transport Security (HSTS) to ensure your connection to UIDAI servers remains encrypted and defend against attacks that attempt to downgrade to an unsecured HTTP. (Man in the middle attack)
2. **Safeguarding biometric data:** Prevent substitution attacks by avoiding the storage of biometric templates (attacker can overwrite template with its own). Instead, use biometric encryption to link a cryptographic key to the biometric data, ensuring neither the key nor biometric data can be retrieved.
3. **Masking:** UIDAI servers keep frequently used data and encryption keys in memory caches, which can be targeted by attacks that reveal these keys. Masking counters this threat by splitting the data into several parts and hiding them. It avoids manipulation of sensitive data directly by an attacker, rather manipulating a sharing of it.

4.TELECOMMUNICATION SECTOR- Security for telecommunications networks and services should ideally follow internationally recognized standards. Following are some measures to enhance network security –

1. **Access and authorisation:** Transmission Terminal Equipment (TTE) should use protocols that ensure mutual authentication and apply the latest cryptographic controls for security. Management traffic needs to be safeguarded with these controls, and TTE systems should have Role-Based Access Control (RBAC) with at least three user roles to handle access and permissions effectively.
2. **Protection against brute-force attacks**: TTE systems must implement measures to protect against brute force and dictionary attacks, such as introducing delays for incorrect password attempts, blocking accounts after multiple failed attempts, using blacklists for weak passwords, and employing CAPTCHA. For enhanced security, at least two of these methods should be used.
3. **Software security**: TTE systems must verify software updates using cryptographic methods like digital signatures and valid code signing certificates to ensure the updates

are genuine. The system should check these updates against a list of authorized public keys or certificates to confirm they come from trusted sources.[15]

FIGURE 5: Defence in depth strategy for cyber security[16]

[15] 'ITSAR203082209.Pdf' <https://nccs.gov.in/public/itsar/ITSAR203082209.pdf> accessed 4 September 2024.
[16] 'CyberSecurityConclaveAtVigyanBhavanDelhi_1 (1)' (n 5).

CHAPTER 3: CONCLUSION & SUGGESTIONS.

In conclusion, in our increasingly digital world, safeguarding public sector networks is vital. Addressing vulnerabilities in finance, administration, healthcare, and telecommunications is essential as the frequency of cybersecurity incidents rises. Strengthening protection in these areas is crucial for maintaining the integrity and trust in public services.

In India, public sector networks are critically vulnerable to cyber threats. The financial sector struggles with phishing and malware issues, exemplified by the Cosmos cooperative bank breach. Healthcare faces frequent attacks, as demonstrated by the AIIMS ransomware incident, while the Aadhaar system has suffered from breaches due to poor security. The telecommunications sector also experiences significant risks, with recent breaches exposing vulnerabilities like SQL injection.

To protect India's critical public sector, financial institutions should upgrade threat monitoring, healthcare must secure devices and manage vulnerabilities, Aadhaar needs enhanced data protection, and telecommunications should enforce strict access controls. These measures will bolster network security across sectors.

It is suggested for public sector organisations to follow the preventive, detective and corrective measures as mentioned under 2.3, some additional suggestions as per the research work done for this project are as follows:

1. **Education and Regular Training:** Indian Public Sector Organisations face a lack of basic cybersecurity knowledge and skills, leading to security breaches like the Aadhar incident. Regular training programs, including emerging threats, should be implemented to ensure all personnel are equipped with the necessary skills.
2. **Sector-Specific Solutions:** While security measures may overlap, each sector (e.g., financial, healthcare) has unique vulnerabilities requiring tailored approaches. This includes handling sensitive data like PII (Personally Identifiable Information) in finance and PHI (Protected Health Information) in healthcare, with sector-specific standards and regulations.
3. **Emphasis on Implementation**: Outdated protocols and poor incident response are common in Public Sector Organisations. To mitigate these issues, organisations need regular security assessments, updates, and well-defined incident response plans that outline roles and responsibilities.

4. **Post-Incident Response Strategies:** A strong incident response plan is essential. Post-incident actions, such as resetting passwords and updating systems, are crucial to recovery. Lessons learned should drive regular system updates to prevent future incidents.

These suggestions aim at strengthening the capabilities of Public Sector Organisations to establish a robust network security framework with preventive, detective and corrective capabilities.

BIBLIOGRAPHY

1. '13 Lakh Cyber Attacks Hit Indian Banks in 10 Months; Who Is behind Them? - India Today' <https://www.indiatoday.in/diu/story/cyber-attacks-hit-indian-banks-rbi-report-swift-network-2481951-2023-12-29> accessed 2 September 2024

2. 'Aadhaar Data Breach — How Sensitive Data Of 1.3 Billion Indians Was Compromised | by Rithik V Gopal | The Deep Hub | Medium' <https://medium.com/thedeephub/aadhaar-data-breach-how-sensitive-data-of-1-3-billion-indians-was-compromised-cb01d0c2d7d3> accessed 11 September 2024

3. Awasya BS, 'Guidelines on Information Security Practices for Government Entities'

4. Balaji DrP and others, 'Cyber Attack - Envenom in Indian Healthcare – A Review' (2023) 4 International Journal of Research Publication and Reviews 1262

5. 'Case Study : 2018 Pune's Cosmos Bank Cyber Attack | by DHARM PATEL | Medium' <https://medium.com/@20dcs071/case-study-2018-punes-cosmos-bank-cyber-attack-cafd221cac25> accessed 11 September 2024

6. 'Cyber Security: Over 1 Lakh Cyber Security Incidents in Govt Organisations This Year - The Economic Times' <https://economictimes.indiatimes.com/tech/technology/over-1-lakh-cyber-security-incidents-in-govt-organisations-this-year/articleshow/102362589.cms?from=mdr> accessed 1 September 2024

7. 'CyberSecurityConclaveAtVigyanBhavanDelhi_1 (1)'

8. 'India's Healthcare Sector Top Target of Cybercrimes: Report - India Today' <https://www.indiatoday.in/india/story/healthcare-sector-top-target-of-cybercrimes-hacking-aiims-icmr-2561733-2024-07-03> accessed 11 September 2024

9. 'ITSAR203082209.Pdf' <https://nccs.gov.in/public/itsar/ITSAR203082209.pdf> accessed 4 September 2024

10. 'P17507500a843000d099250f19a00b04019.Pdf' <https://documents1.worldbank.org/curated/en/099081723223525669/pdf/P17507500a843000d099250f19a00b04019.pdf> accessed 11 September 2024

11. '(PDF) Review of SQL Injection : Problems and Prevention' <https://www.researchgate.net/publication/325940419_Review_of_SQL_Injection_Problems_and_Prevention> accessed 11 September 2024

12. 'Telecom Turmoil – Cybersecurity Emerges as Top Priority amidst Rising Threats | Communications Today' <https://www.communicationstoday.co.in/telecom-turmoil-cybersecurity-emerges-as-top-priority-amidst-rising-threats/> accessed 11 September 2024

13. 'Threat Actor Breaches BSNL Server Database, Puts up Dataset on Dark Web | Company News - Business Standard' <https://www.business-

standard.com/companies/news/threat-actor-breaches-bsnl-server-database-puts-up-dataset-on-dark-web-123122200310_1.html> accessed 11 September 2024

14. 'What Is Network Security? The Different Types of Protections - Check Point Software' <https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/> accessed 2 September 2024