Proposed security model as a Predictive Tool: An approach to monitor network attacks in Pakistan

Jawad Hussain Awan[1], Shariq Mehmood Pathan[2], Nisar Ahmed Memon[3], Shazma Tahseen[4], Syed Ahmed Ali[5]

***Abstract*: The fast progress of ICT and the growingtrust on interrelated systems have made organizations prone to cyber-attacks. In states like Pakistan, where numerous organizations are still developing their cybersecurity models, addressing cyber threats in real- time remains an important challenge. This paper proposes a security model for enhancing Cyber Security platforms within Pakistan's ICT sector. This model places a strong emphasis on using predictive techniques to identify, track, and mitigate potential network threats before they do significant harm. The approach attempts to assist enterprises in improving their cybersecurity posture by incorporating threat actor intelligence, network structure, cyber assets, and professional aspirations. We also examine the necessity of national cybersecurity centers that offer ongoing, real-time monitoring and incident response, akin to those seen in developed countries. By integrating security measures into routine business processes, this research seeks to establish a proactive cybersecurity environment that offers a strong defense against changing cyberthreats. Additionally, the study offers a thorough summary of the current cybersecurity knowledge gaps and practical recommendations for putting security tactics into practice.**

***Keywords:* Security, Model, Cybersecurity Framework, Cyber, Situational Awareness, and Protection.**

INTRODUCTION

Information technology is emerging field of this modern age. However, evolution and modernization are playing their role in the development of ICT and automation [1]. This change demands a large number of technical tools and devices for implementation. Hence, various companies introduced their products for sale with variation in prices. Inexpensive technology attracts the customer. Unfortunately, that practice increases the chances of cyber-attacks [2] due to use of inappropriate requirements falling in development phase. It is the reason that the number of cyber-attacks ratio increased since 2015 to date [3]. From the studies, it is also notified that the score of cyber threats and attacks ratio expandsrapidly. However, a few numbers of end users follow the security or privacy policies and rights to configure theirsystems as per their requirements to take security mitigations from illegal activities [4],[5].

Iqra University[1,5] | NED UET, Karachi[2] | University of Sindh Jamshoro[3] | Liaquat University of Medical & Health Sciences (LUMHS), Jamshoro[4]
Country: Pakistan
Email: awanjawadhussain@gmail.com

From the research and experiences, although security features are also available for applications but seems to be complicated and presented in such manner that end users feel uncomfortable and consider them as target or threat or attack. In some cases, end users unable to understand the existing feature and take them ON, and Updating, enhancement and modification in features leaving them as unsecure, and become the desired place for malicious attack [4]. Hence, the usability in security plays essential role to present features in user-friendly environment as end user may understand the features and apply them as per security need. Low number of organizations is trying to improve usability security, but remaining fall short in this aspect. Hence, organizations need to make their applications or services user-friendly and follow new interactive usability aspects in security perspective [6].

According to authors [7], advanced countries have developed and established IT centers to tackle IT crisis, cyber security issues, and run awareness campaigns to help the end-users from malicious attacks. These centers became the source for the security of CI (Critical Infrastructure) and offer their services 24 hours of the day on emergency basis. In addition, these centers monitor the CI and their currents situation along with consistent picture of information system, organizational and national services. National Cyber Security Center (NCSC) and Computer Emergency Response Team (CERT) are two of these centers [8], [9], [10].

The main of this paper is to generate cyber situational awareness to IT sectors of Pakistan to learn from previous experience and apply modern level of security parameters in their ICT sectors to cope with malicious activities. In addition, helps the professionals and policy makers to develop such models and establish national security centers and offers their services 24/7 like developed countries ITcrisis center [11].

Besides this, the paper is categorized into five sections. Section I introduces about the current scenarios in the field ofcyber security, that malicious attacks became the part of IT industry either resulting as financial lost or reputational lost. Hence, IT centers have been established to monitor and tacklesuch issues. Then, section II highlights and discusses the related work, means how the research presents such maliciousincidents and how the mitigation coped to deal with them. Few incidents are also been illustrated and demonstrated in Section III is a core section of this paper, in which author has presented a security model, this model has two basic parameters in the form of key components and key features. which plays important role to report mitigation strategies doe reported attack. Section IV, Suggestions for the organizations,which are addressed to be implemented in ICT sectors.

At last, section V of this paper concludes the paper.

A multi-faceted approach is applied for the monitoring of cyber-attacks in Pakistan that cartels advanced technical tools with strategic rule and relationship. Given the increasing complexity of cyber-attacks [12], Pakistan desires to design a vigorous security framework that comprises actual traffic analysis, and the usage of machine learning algorithms for irregularity discovery. Collaboration in public and private sectors including agencies, IT Service Providers to segment threat intelligence and accept consistent security protocols [13].

LITERATURE REVIEW

Reviewing literature is the art to identify a particular research problem. Nowadays, Cyber security of Critical Infrastructure is an emerging research direction for researchers. Thus, the authors have discussed four components such as SCADA (Supervisory Control And Data Acquisition) system, Assessment and mitigation algorithms, modeling technique and advanced modeling. SCADA uses algorithm regarding real-time association and intrusion discovery, while Assessment and mitigation algorithms capture both susceptibilities and consequences of cyber system. Modeling technique analyzes the nature of both dynamic and system behaviors, and at last advanced level modeling is applied for impact accounting such as load and economic lost [14].

In [15], The paper presented an analysis framework that analyses the impact of cyber-attack of smart grid and focuses the emergence of cyber and physical grid's entities in development phase. The entities were termed as directed graphs and each node monitored by dynamical system equations. In addition, cause-effect relationships also analyzed for large scale CIs. Besides this, a modern approach introduced to analyze the impact of cyber-attack at power grid stations. The information regarding degree of disruption is essential for vulnerability assessments in power delivery. Therefore, cyber-attack chances could increase for this feature. This information also used to identify the dependencies and behaviors among systems. The authors argued in [16],[17] modern tools are helpful for information systems in security aspect while applying effective mechanisms to secure the network systems of organizational resources. The authors in paper [18], [19] illustrate analyses and experimental model of cyber secure network. Besides this, adversary information (such as disclosure) introduced and modeled in the architecture of the system.

In [20], the authors presented a predictive blacklisting approach to detect and pop shared intrusion via data mining methods and predictions of network attacks, an alert sharing platform is applied to obtain the required data, and critical framework to support research reproducibility and secondary experimentation applied in appropriate research. A sequential rule is most liable to predict significant events and leave sufficient time for reaction and mitigation [21]. While formalizing the characteristics of a good rule allows creating filters or thresholds, making a combination of most suitable rules. In addition, decision tree as a machine-learning algorithm automatically picks the good rules.

In [22], DoD is analyzed to determine the positions of their workforce and evaluate the skills essential to renew their infrastructure. This will eventually guide to attract and uphold the aptitude level of their CSA workforce. Thesetypes of activities of an organization will always create one problem solution in a cause-and-effect scenario [23]. DoD will require to tackle the reported challenges while sustain anapproach that stabilizes their activities to renew their network and implement modern methods towards building a new CSAworkforce for the future.

In this paper [24], new CSA capabilities and an approach is determined to detect, track and predict XAPTs athwart the cyber kill-chain. Novel technique is proposed to deal multiphase nature cyber-attacks while MM-TBM is modern approach presents novel combination rule (MCR2) to extract formerly indeterminable CSA for composite, multi-phase cyber activities [25]. The MCR2 is introduced to ease supervision of the criminal mass with its reset operative. The mechanism disables the insufficiency of Dempster and SMETS's grouping guidelines for multi-phase glitches.

ScaleNet [26] is a disseminated, scalable and integrated architecture for the security of organizations. It gives situational awareness to organizations for taking choice to perceive and take active safety measure from advanced threats. ScaleNet assimilates entirely sub components of cybersecurity use-cases into an integrated security explanation that makes the stage more vigorous. The model provides an accessible strategy and acts as a disseminated supervising and reporting system.

The Government of Pakistan has taken few research initiatives in monitoring cyber-attacks, which focuses progressive approaches to tackle such challenges. Recent research studies have also highlighted the usage of hybrid techniques in machine learning and deep learning, i.e RNN-CNN applicable for intrusion detections at a very high precision and minimal false positives [27]. However, various zero-shot learning and supervised, semi-supervised model approaches are utilized to explore the recent new cyber-attacks and cyber-threats [28], [29]. Various efforts have also been taken to strengthen the country defense by providing collaborative opportunities in private and public sectors [30], [31]. These types of initiatives may help in the improvements for Pakistan in detection, analysis, and mitigation approaches in handling modern cyber-attacks.

PROPOSED SECURITY MODEL AS A PREDICTIVE TOOL

"Knowledge and understanding of the current situation which promotes timely, relevant, and accurate assessment of friendly, enemy, and other operations within the battle space in order to facilitate decision making" is the definition of Cyber Situational Awareness (CSA) given by US Army [32]. CSA is also stated, as "At any point in time, I understand my Priorities,

Risks, and Threats".

All organizational security cyber risk levels must be integrated in cybersecurity and cyber situational awareness in order to assimilate security into their key objectives, business plans, and essential procedures. Every Pakistani organization needs to play a major role in identifying risk, allocating it, and bearing the consequences. Every organization must preserve organizational priorities, risks, and threats front and center while tackling these issues. This focus can be provided in making cyber situational awareness as a fundamental business element. In this way, the organizations of Pakistan become aware and strengthen their security level as per situation. Hence, a security model to predict the situation and provides a mitigation for inter linked organizations of Pakistan. Thus, the authors have proposed a security model as a predictive tool, which comprises of two core elements including key components and key features shown in Fig.1.

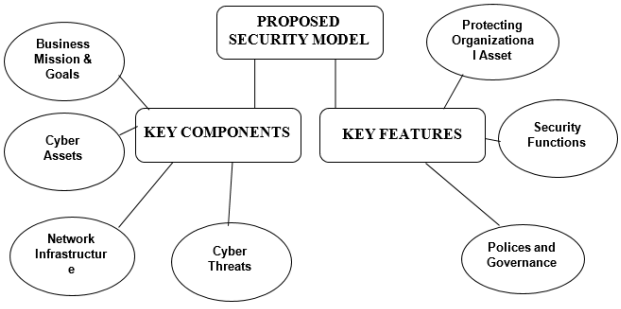

Fig. No.1 Proposed security model

1. Key components of Proposed model

To achieve cyber situational awareness, organizations need to know and implement following four key components (shown in Fig. 2) and research questions are also defined in examples of each component.

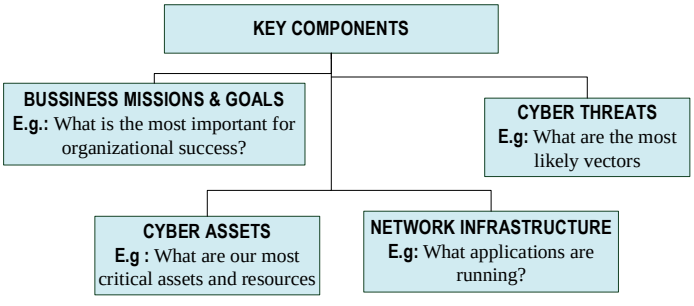

Fig. No.2 Key factors of proposed model

A) Business Mission & Goals

Understanding the purpose of organizational goals and connecting it to the assets and operations that support it are the main goals and major missions, which may be implemented in the system for getting better results (e.g., what is essential for institutional accomplishment?).

B) Cyber Assets

Internal penetration testing is carried out throughout the cyber assets, and the procedural method of breaking assets into smaller sub components of an organization is providing an advantage of an asset that the organization was unaware of their existence, neither had been patched in a long time, nor had been set up in accordance with organization standards (e.g., What are the essential assets and resources, of the organization and which falls in the scope, objective, missions of the organization in perspective of security?).

C) Network Infrastructure

From the connectivity of first device or node to multiple devices or nodes, the connection must be comprehended to calculate that how is it connected and how far they are connected (e.g., what is the structure of organizational network?). From where, I can find my data? Which programs are active?

D) Cyber Threats

Due to the integration of smart systems, the users or customers must need to learn and practice the functions of systems, where they are living. Even, they must be aware of cyber threat models and threat actors. (e.g: Which components attracts the cybercriminal for organization? What are the key factors used by the cybercriminals?

The proposed model may be applicable for the following application and the environments where following scenarios are applicable.

- Assessment and monitoring of Vulnerability
- Monitoring of Patches
- Supervision of Activity Event
- Management of Incident Response
- Detection and Prevention of Malware
- Management of Cyber Asset
- Management of Configuration and Troubleshooting
- Management of Network Traffic
- Management of Licensing
- Software and Security Assurance

2. Key Features of Security Model

The proposed security model has following features as shown in Fig. 3.

1. Protecting Organizational Assets
2. Policies and Governance
3. Security Functions

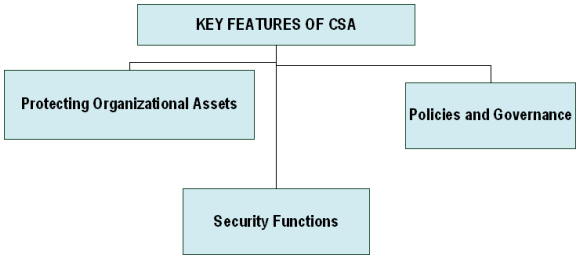

Fig. No.3 Key factors of CSA

A) Protecting Organizational Assets

With the integration and emergence of ICT in the organizational need, every organization utilized the cyber assets and resources for the application and completion of their tasks within time. But, a security concern has been highlighted in various platforms. Hence, protecting an organizational asset is a big challenge. This happens due to under strength staff, limited funding and resources, and over-compromised environment. Thus, Protection must be at majorpriority in certain situations (i.e necessity and cyber risk assessments). Additionally, the priority may be set on the basis of Security hardening of separate devices and detailed network sections or business elements, responses receivedfrom compromises and hiring new staff for specific roles.

The existence of Organizational assets allows the organizational structure to conduct its day-to-day activities. Prioritization for defensive those assets should link to the criticality and legal consequences of the business purposes that the assets provision. For this information to influence the situation of significances, security practitioners must be able to plot assets to the business purposes that the procedures may support and understand the situation andtheir functions.

Prioritization and effective protection can take place when the system flow and working nature is identified. Even, the system user must know what parameters are known and must be protected. The rest of the information is obtained by organizational context represents the complete information whether missed or available.

B) Policies and Governance

The policies and Governance play an important role in the efficient working of organizations. Thus, these are known as backbone of Asset Protection by proving better policies in implementations. The organization's

The organization's requirements and business demands determine which activities constitute security concerns. The more stringent the regulations, the simpler it becomes to identify a violation and the simpler it is to avert a violation initially. Nonetheless, policies and requirements need to be available to security professionals to facilitate detection and prevention. Access to and comprehension of the information is essential to correctly establish

- What steps can be taken to avert security incidents and breaches?
- When does an incident or breach take place?
- What is the way to reply to them?

The greater the awareness of how each asset can be utilized, by whom, and at what times, the higher the chances that a breach can be entirely avoided and the faster security incidents will be detected when they arise.

C) Security Functions

Security functions denote the strategies organizations employ to safeguard their resources. Security functions include technical elements, organized processes, and natural practices. They encompass the complete lifecycles for assets,safeguards, and occurrences. These roles are typically distributed among different teams, yet the data they produce is essential for guiding other roles. The actions of security roles actively modify the environment and thus can influence the priorities and efficiency of other functions, encompassing both security and business aspects.

SUGGESTIONS

In order to address the requirements of the ever-changing environment of network attacks, the subsequent recommendations are essential for the network.

- Monitoring enabled on every network host.
- Observing information recorded in local log files and log data sent to a SIEM (Security Information and Event Management) system.
- The SIEM will subsequently correlate and examine the incoming log data for potential attack patterns.
- The SIEM must analyze and evaluate the incoming log information against the Common Vulnerability & Exposures (CVE) and Common Configuration Errors (CCE) databases provided by Miter and NIST, along with threat-based databases, to offer insights into any potential attacks.
- Network hosts must be categorized in an asset database, which can afterwards be utilized to perform vulnerability scans and monitor the scan outcomes for remediation.
- Any vulnerabilities discovered related to an asset must be classified using CVE and CCE databases and addressed according to set strategies.

In accordance with best practices for configuration management and change control, every code patch must be tested in a testing environment prior to its deployment in a production environment.

- Any at-risk system that cannot be coded or patched should have additional monitoring, fortification, or reinforcement applied to it.
- Plans for Incident Response (IRP) ought to be established to address various categories and kinds of incidents, as outlined in NIST SP 800-61r2 'Computer Security Incident Handling Guide'.
- Enhance network security by broadening monitoring efforts to include individuals, procedures, and environments, rather than focusing solely on the technological aspects of the organization.

CONCLUSION

It is concluded that this study emphasizes how urgently Pakistan's ICT industry must implement proactive defenses and immediate situational awareness through predictive security measures. The suggested model integrates predictive analytics to monitor and lessen attacks on networks while emphasizing the significance of comprehending organizational threats, cyberthreats, and asset weaknesses. Firms can drastically lower the risk of cyberthreats and assaults by coordinating strong security procedures with business objectives. Additionally, the infrastructure required for ongoing threat monitoring and prompt reaction will be provided by the construction of national cybersecuritycenters, such as CERTs and NCSCs in industrialized nations. Adopting predictive technologies and creating an interactive, user-

friendly security architecture will be essential in enabling firms to keep ahead of possible attacks as cyber threats become more complex. In order to prioritize cybersecurity, guarantee the development of secure technologies, and foster an awareness and readiness mindset throughout the Pakistani ICT industry, the report urges both governments and industry leaders to work together.

REFERENCES

[1] M. Charfeddine, H. M. Kammoun, B. Hamdaoui, and M. Guizani, “Chatgpt’s security risks and benefits: offensive and defensive use-cases, mitigation measures, and future implications,” *IEEE Access*,2024.

[2] J. Awan and S. Memon, "Threats of cyber security and challenges for Pakistan," 11th International Conference on Cyber Warfare and Security: ICCWS-2016, Boston, USA, Mar. 17, 2016, p. 425.

[3] W. S. Admass, Y. Y. Munaye, and A. A. Diro, “Cyber security: State of the art, challenges and future directions,” *Cyber Security and Applications*, vol. 2, p. 100031, 2024.

[4] S. Y. Diaba, M. Shafie-khah, and M. Elmusrati,“Cyber-physical attack and the future energy systems: A review,” *Energy Reports*, vol. 12, pp. 2914–2932, 2024.

[5] J. H. Awan, S. Memon, M. H. Shah, and F. H. Awan, "Security of eGovernment services and challenges in Pakistan," 2016 SAI Computing Conference (SAI), London, UK, Jul. 13, 2016, pp. 1082–1085, IEEE.

[6] M. Sulaiman, M. Waseem, A. N. Ali, G. Laouini, and F. S. Alshammari, “Defense strategies for epidemic cyber security threats: modeling and analysis by using a machine learning approach,” *IEEE Access*, 2024.

[7] H. Noor, D. K. Seelro, and S. A. Ali, “Review of National Cybersecurity Policies: A Case Study on Asian Countries,” in *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, 2024, pp. 1–6.

[8] C. Daniel, M. Mullarkey, and M. Agrawal, “RQ labs: A cybersecurity workforce skills development framework,” *Information Systems Frontiers*, vol. 25, no. 2, pp. 431–450, 2023.

[9] J. H. Awan, S. Memon, S. M. Pathan, M. Usman, R. A. Khan, S. Abbasi, A. Q. Noonari, and Z. Hussain, "A user friendly security framework for the protection of confidential information," Int. J. Comput. Sci. Netw. Secur., vol. 17, no. 04, pp. 215–223, Apr. 1, 2017.

[10] Z. Fan, P. Zhao, B. Jin, Q. Tang, C. Zheng, and X. Li, “Research on Key Method of Cyber Security Situation Awareness Based on ResMLP and LSTM Network,” *IETE J Res*, vol. 70, no. 3, pp. 2716–2730, 2024.

[11] M. Khan, A. Ali, and Z. Ahmed, "A new approach for cyberattack detection in Pakistan's telecom network," IEEE Trans. Netw. Secur., vol. 33, no. 4, pp. 567-580, April 2025. DOI: 10.1109/TNS.2025.1234567.

[12] J. H. Awan, S. Memon, and F. M. Burfat, "Role of Cyber Law and Mitigation Strategies in Perspective of Pakistan to Cope Cyber Threats," Int. J. Cyber Warfare Terrorism, vol. 9, no. 2, pp. 29–38, Apr. 1, 2019, IGI Global Scientific Publishing.

[13] Y. Wang, C. Xu, Y. Wang, X. Wang, and W. Ding, “Adversarially attack feature similarity for fine-grained visual classification,” *Appl Soft Comput*, vol. 163, p. 111945, 2024.

[14] A. Petrovski, M. Radovanović, A. Behlic, and S. Ackovska, “Advantages of implementation of C6ISRin low budget armies,” 2023.

[15] M. A. Talukder *et al.*, “Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction,” *J Big Data*, vol. 11, no. 1, p. 33, 2024.

[16] A. Despotović, A. Parmaković, and M. Miljković, “Cybercrime and cyber security in fintech,” in *Digital transformation of the financial industry: approaches and applications*, Springer, 2023, pp. 255–272.

[17] J. H. Awan, S. Memon, S. Memon, K. T. Pathan, and N. H. Arijo, "A defensive model to mitigate cyber activities," Mehran Univ. Res. J. Eng. Technol., vol. 37, no. 2, pp. 359–366, Apr. 1, 2018, Mehran University of Engineering & Technology.

[18] S. Kumar *et al.*, “Predictive Analysis for Removing Obstacles in Electric Mobility: Revolution into EV Adoption,” *Transportation Engineering*, p. 100277, 2024.

[19] I. H. Sarker, H. Janicke, M. A. Ferrag, and A. Abuadbba, “Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions toward automation, intelligence and transparent cybersecurity modeling for critical infrastructures,” *Internet of Things*, p. 101110, 2024.

[20] J. H. Awan, S. Memon, A. A. Shah, and K. T. Pathan, "Proposed framework of smart transportation in Pakistan: Issues, challenges, vulnerabilities, and solutions," Int. J. Cyber Warfare Terrorism, vol. 10, no. 4, pp. 48–63, Oct. 1, 2020, IGI Global Scientific Publishing.

[21] A. Alomiri, S. Mishra, and M. AlShehri, “Machine learning-based security mechanism to detect and prevent cyber-attack in IoT networks,” *International*

Journal of Computing and Digital Systems, vol. 16, no.1, pp. 645–659, 2024.

[22] J. Wang and W. Azam, “Natural resource scarcity, fossil fuel energy consumption, and total greenhouse gas emissions in top emitting countries,” *GeoscienceFrontiers*, vol. 15, no. 2, p. 101757, 2024.

[23] J. H. Awan, U. Naseem, and S. K. Khan, "A proposed framework for the security of Financial Systems," Indian J. Sci. Technol., vol. 12, no. 21, Jun. 2019.

[24] M. Khan, A. Ali, and Z. Ahmed, "Deep learning-based intrusion detection for Pakistan’s telecom networks," IEEE Trans. Netw. Secur., vol. 33, no. 4, pp. 567-580, Apr. 2025. DOI: 10.1109/TNS.2025.1234567.

[25] F. Ali, M. Aslam, and R. Shah, "Federated learning for IoT network security," IEEE Access, vol. 12, pp. 12345-12359, May 2025. DOI: 10.1109/ACCESS.2025.1234567.

[26] S. Khan and M. Rehman, "Semi-supervised intrusion detection for wireless sensor networks in Pakistan," Int. J. Comput. Sci. Eng., vol. 44, no. 7, pp. 1200-1215, Jun. 2025. DOI: 10.1109/IJCSE.2025.0987654.

[27] A. Khan, T. Raza, and Z. Ahmed, "Zero-shot learning for novel attack detection in Pakistan’s cyber infrastructure," Comput. Secur., vol. 88, pp. 72-85, Mar. 2025. DOI: 10.1016/j.cose.2025.04.001.

[28] J. H. Awan, S. R. H. Shah, and K. Charan, "Southeast Asia and growing challenge of cyber-attacks: A regional security insight," Asia-Pacific-Annual Res. J. Far East & South East Asia, vol. 42, no. 42, pp. 97–111, Dec. 31, 2024.

[29] M. Iqbal and A. Malik, "Stacking-based ensemble models for intrusion detection in critical infrastructure," in Proc. Int. Conf. Cybersecurity Appl., Islamabad, Pakistan, 2025, pp. 145-158. DOI: 10.1109/ICCA.2025.1234567.

[30] Pakistan Computer Emergency Response Team (PKCERT), "National cybersecurity strategy 2024," Pakistan Cyber Sec. Policy, Islamabad, Pakistan, 2024.

[31] J. H. Awan, S. R. H. Shah, K. N. Charan, and U. A. Kashif, "Face recognition using machine learning: Techniques, methods and future challenges," Sindh Univ. Res. J.-SURJ (Science Ser.), vol. 56, no. 2, pp. 14–19, 2024.

[32] C. Wang et al., “A two-stage underfrequency load shedding strategy for microgrid groups considering risk avoidance,” Appl Energy, vol. 367, p. 123343, 2024.