Tackling Pakistan's Cyber Security Challenges: A Comprehensive Approach

Muhammad Ibrar[1], Hang Li[1], Jiachi Wang[1], and Shahid Karim[2]
(Corresponding author: Hang Li)

Software College, Shenyang Normal University, Shenyang, China[1]
Shenyang 110034 China
Research & Development Institute of Northwestern Polytechnical University in Shenzhen[2]
Shenzhen 518057, China
Email: lihangsoft@163.com

(Received Dec. 26, 2022; Revised and Accepted Apr. 16, 2023; First Online Apr. 30, 2023)
The Special Issue on Computational Intelligence Networks for Privacy and Security in Evolving Internet of Multimedia Things
Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

The rapid growth of internet usage and its various applications, such as banking, shopping, social networks, and other business-related activities, has moved people closer to cyberspace. The implications of this growth have also come to Pakistan, where cyber security and threats are becoming an essential aspect of cyberspace. This paper will discuss the challenges Pakistan faces regarding cyber security and the steps that need to be taken to address those threats. It will focus on the recent cyber-attacks, such as ransomware and distributed denial-of-service (DDoS), which have disrupted vital services in Pakistan. Furthermore, it will discuss the potential solutions and strategies that can be used to ensure that all users in Pakistan have a secure experience when accessing the internet. Finally, it will also present recommendations for organizations to consider when developing cyber security policies for their operations in Pakistan.

Keywords: Challenges for Pakistan; Cyber Security; Cyber Security Policies; Cyberspace

1 Introduction

Cyber Security is the practice of protecting systems, networks, and programs from digital attacks. These attacks usually aim to access, change, or destroy sensitive information, extort money from users, or interrupt normal business processes [15]. Cyber security involves the prevention of, detection of, and response to security incidents that take place in a digital environment [22, 23]. It is a rapidly evolving field that is becoming increasingly important today [5, 24]. The amount of data created and stored online increases each year. This growing quantity of data increases the risk of cyber-attacks as hackers look for opportunities to exploit it. Organizations must put in place various measures to protect their confidential information and prevent malicious actors from gaining unauthorized access or disrupting their operations [17].

Pakistan is one of the developing countries where cyber security is yet to gain momentum due to a lack of awareness, expertise, and resources available for this purpose. The country faces challenges ranging from a lack of technical capacity to develop and implement effective cyber security strategies, a lack of legal framework, an absence of public-private partnerships, and funding constraints [4]. In addition, Pakistan also faces several social challenges, such as low levels of education, poverty, and a lack of access to technology, making it difficult for people to protect themselves from cyber threats. Furthermore, due to its proximity to volatile countries such as Afghanistan and Iran, Pakistan is also at risk of becoming a target for cyber-attacks by state-sponsored hackers [7]. The government has taken several steps to address these challenges, such as establishing the Cyber Emergency Response Team (CERT), which monitors the country's IT networks and responds to any cyber threats it detects. The government also provides awareness campaigns to educate people about cyber security threats and how to protect themselves online as shown in Figure 1.

However, these efforts are just a drop in the ocean, considering the scale of the problem. The country needs to develop more comprehensive policies and strategies on cyber security to combat the threat posed by cybercriminals effectively [8].

With the world increasingly becoming interconnected through technology, the threat of cybercrime is also on the rise. As a result, countries worldwide are making great strides to increase their cyber security measures to prevent cyberattacks and data breaches. Pakistan is no exception. The government is constantly grappling with

Figure 1: The theoretical concept of national security

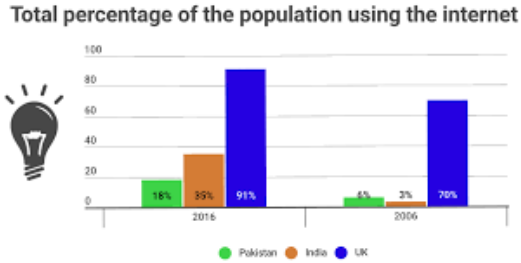

Figure 2: Population using the internet in Pakistan, India, and UK

various cybersecurity challenges, from the risk of malicious actors exploiting its networks and infrastructure to the need to update critical information systems and protect citizens data [15].

The percentage of the population using the internet in Pakistan, India, and the UK is shown in Figure 2. In recent years, Pakistan has made some critical reforms to improve its cyber security. In 2019, the Ministry of Information Technology and Telecommunications launched the National Response Centre for Cyber Crimes (NR3C). This center has been instrumental in increasing awareness about cyber threats and coordinating efforts between law enforcement and other relevant agencies on cybercrime investigations. The center also develops training materials for law enforcement officers and raises public awareness about cyber safety and security best practices [9].

The government has also enacted several laws to help protect against cybercrime. In August 2020, the National Assembly passed the Prevention of Electronic Crimes Act (PECA) 2020, which criminalizes various activities, including hacking, fraud, intellectual property rights infringement, terrorism, extortion, and identity theft. The government has also issued guidelines for protecting the personal data of individuals, including measures to prevent unauthorized access or disclosure [10]. Despite these efforts, several challenges remain that need to be addressed to ensure a secure cyberspace in Pakistan for example, adequate resources and personnel to be improved to investigate cyber threats and enforce cyber laws. In addition, there are areas for improvement in existing legal frameworks that make it challenging to pursue sophisticated cybercrime cases. Furthermore, the country's critical infrastructure remains vulnerable to attack due to outdated technology and weak security measures. Finally, there is a need to develop comprehensive policies and strategies that address both domestic and international threats [11].

Overall, it is clear that Pakistan still faces a range of cyber security challenges. However, by taking steps such as improving laws and regulations, strengthening infrastructure protection measures, and enhancing collaboration between relevant stakeholders, the country can make progress toward achieving a safe and secure cyberspace for its citizens.

2 Research Question

What strategies can be used to improve cyber security in Pakistan and address the challenges faced by the country in this regard?

3 Research Objectives

1) To measure the levels of cyber security in Pakistan and assess the current efforts to mitigate the risk of cyber-attacks.

2) To identify and analyze the critical challenge of cyber security in Pakistan and suggest ways to strengthen the existing protection infrastructure.

3) To assess the extent to which Pakistani businesses are vulnerable to cyber threats and suggest measures for their protection.

4) To investigate the government's and other stakeholders' role in promoting cyber security in the country.

5) To understand the various tools and technologies hackers use to penetrate Pakistani networks and devise practical solutions to combat them.

6) To evaluate the preparedness of Pakistan to counter emerging threats posed by cybercriminals, such as phishing and malware attacks.

7) To examine the efficacy of existing international laws, regulations, and practices in safeguarding Pakistani networks from external cyber threats.

8) To develop an effective strategy for raising public awareness of cyber security in Pakistan and suggest necessary steps for its implementation.

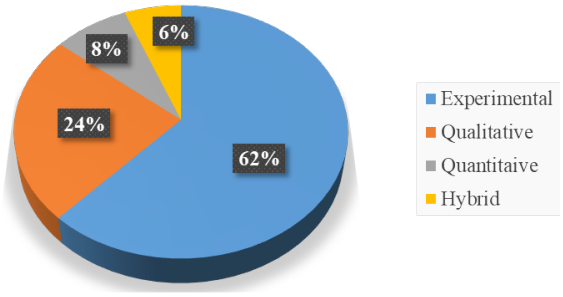

Figure 3: Distribution of articles according to methodology

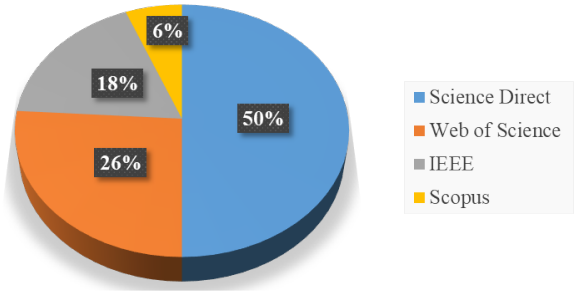

Figure 4: Distribution of articles according to the percentage of databases

4 Research Problem

Cyber security is an increasing concern in Pakistan. The country has faced numerous cyber-attacks, from traditional cybercrime and identity theft to political attacks targeting government and private institutions. Despite the growing cyber security threats, there needs to be more knowledge, awareness, and preparedness among the public and organizations to counter such threats. Moreover, the country needs more adequate laws and infrastructure to combat cybercrime effectively. As such, it is essential to research the cyber security challenges faced by Pakistan and develop strategies to safeguard its citizens and institutions from these threats. This research will focus on identifying the major cyber security threats faced by Pakistan, understanding their impact on the country, analyzing the current strategies adopted by the government to address these challenges, and proposing potential solutions to these cyber security issues.

5 Literature Review

Cyber security is a significant concern today, and Pakistan is no exception. As technology advances, the security of digital systems and networks has become increasingly important in maintaining the integrity of nations and businesses. The prior research for cyber security has been categorized based on research methodology (i.e., experimental, qualitative, quantitative, and hybrid), as shown in Figure 3. Figure 4 displays the percentage of databases containing the number of papers published for cyber security. We have selected four well-known databases to evaluate the statistics for this review. The experience of Pakistan in this regard has been mixed, with some successes and many challenges. This paper will review the existing literature on cyber security in Pakistan, examining the country's main challenges and possible solutions to address these issues [12].

It is essential to understand the scope of the cyber security problem in Pakistan. Over the past few years, several documented cases of cyberattacks originated in Pakistan, and hackers are targeting an increasing number of individuals. In addition, state actors are involved in state-sponsored cyber espionage and other malicious activities. These threats come from both external actors as well as domestic criminals. Furthermore, due to lax regulations on data protection, businesses are more vulnerable to data breaches and cybercrime in general [13]. One of the main challenges faced by Pakistan is the need for a practical legal framework governing cyber security issues. Several laws and regulations exist on the books, but they must be more comprehensive to address all aspects of cyber security. This system has hindered efforts by public and private organizations to address cyber threats with any degree of permanence. Furthermore, enforcement of these laws could be more robust due to a lack of adequate resources or political will [14]. According to [3] modern threats and types of data expected to be attacked are presented in Table 1.

Another critical challenge is more awareness and education about cyber security among citizens and government agencies. People have become increasingly dependent on technology without understanding its associated risks, leading to a higher incidence of online fraud, identity theft, and other malicious activities. Similarly, governmental institutions lack sufficient resources and training to address the challenges cyber criminals pose effectively. Fourth, another major challenge for Pakistan is the need for skilled professionals to protect networks from attackers. While some professionals are currently working in the field, their numbers are insufficient to address the growing problem that Pakistan faces from external actors and domestic criminals [16]. Additionally, there are also numerous challenges related to international cooperation on cyber security issues faced by Pakistan. For example, some countries are unwilling to cooperate with Pakistan due to sensitive information being shared across borders or because they may seek a competitive advantage over Pakistan regarding cyberspace capabilities. Additionally, government agencies in other countries may be unwilling to share information or provide assistance due to security concerns or because they view Pakistan as a potential source of cybercrime or terrorism [18]. While there have been some successes in addressing cyber secu-

Table 1: Modern threats and types of data expected to be attacked

Threats	Domains
Surveillance	Social, E-commerce, environment, and political governance
User Profile	Actives and behavioral characteristics
Cyberstalking	Harassment and intimidation
Clickjacking	Press the link or like button, move cursors, use the camera and microphone
Location Privacy	Geotagging
Identity profile cloning	Creating a fake profile
Information Leakage	Health, infrastructure, operational, and intellectual property information
Fake profile Attacks	User information
De-anonymization	Health services, social media, and E-commerce trades
Inference Attacks	Prediction Sensitive, political, religious, and educational information

rity threats in Pakistan, numerous challenges still need to be addressed before meaningful progress can be made. These include a lack of adequate legal frameworks and enforcement mechanisms; inadequate public awareness; insufficient numbers of skilled professionals; and difficulty with international cooperation on cyber security issues. With improved governance and better regulations, Pakistani citizens and businesses can be better protected from cyber threats.

6 Theoretical Framework

Cyber security is the collective set of activities intended to protect computers, networks, programs, and data from unauthorized access, exploitation, and disruption. Pakistan is no stranger to cyber threats. As a rapidly developing economy, the country faces various cybersecurity challenges due to its limited capacity to handle sophisticated cyber-security threats, weak policy frameworks, and limited access to technology and know-how for proactive security measures. The cyber security challenge faced by Pakistan is multi-faceted, as it involves both state and non-state actors who use the internet for criminal activities, espionage, hacking, and manipulation of information. In particular, the country has been subject to frequent cyber-attacks from state actors in the region and abroad. Furthermore, Pakistan faces challenges from cybercrime, ranging from fraud and hacking to identity theft and phishing. As more organizations increasingly connect to the internet and rely on digital systems for their operations, they face an increased risk of becoming cyber-attack targets [19]. To address these challenges, effective policy measures that promote cyber security amongst organizations operating in Pakistan need to be established. There is a need to develop a comprehensive regulatory framework that will ensure the safety of digital systems and networks. Furthermore, organizations must invest in effective cyber security measures such as firewalls and encryption technologies to protect their systems from threats. Additionally, organizations should adopt effective incident response plans that will enable them to address any incidents occurring due to cyber security threats quickly [20].

Organizations must invest in capacity-building initiatives to develop adequate cybersecurity capabilities and provide technical assistance for properly implementing security measures. Additionally, Pakistan must work closely with regional and global partners on international forums such as the United Nations Group of Governmental Experts on Cyber Security (UNGGE) to coordinate better efforts to enhance its cyber security capabilities [21]. At a national level, initiatives such as awareness campaigns must be undertaken to educate individuals on their role in maintaining existing levels of cyber security. Such efforts can improve Pakistan's security by encouraging citizens and organizations to adopt proactive measures against threats.

7 Cyber Design Structure

1) Understand the fundamentals of user experience design: User experience (UX) design is a process for understanding how users interact with digital products and services to improve usability, satisfaction, and efficiency. It includes researching user needs designing and visual elements such as visuals, animations, illustrations, and other graphical elements that enhance the user's experience.

2) Develop a security-first mindset: Security is integral to cyber design since it helps protect users from malicious threats or data theft. By creating secure designs and processes from the ground up, you can help ensure that your product or service meets industry best practices for keeping users safe online.

3) Establish innovative-cation protocols: Authentication protocols are vital when protecting sensitive data stored on a system or website. An exemplary cation protocol should combine factors such as passwords, biometrics, two-factor authentication (2FA), URL scanning checks, and captcha challenges to bust

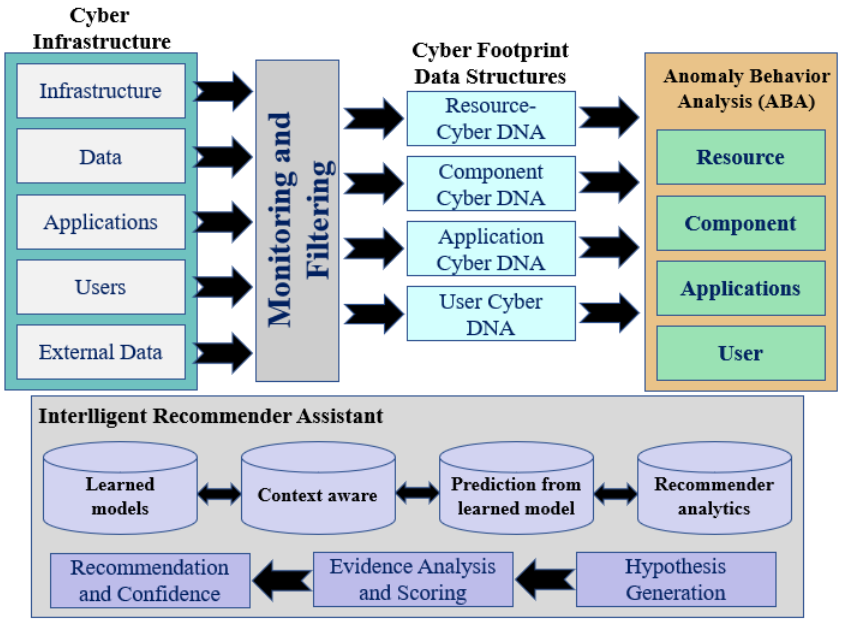

Figure 5: Intelligent Cyber security assistant architecture ***The figure did not cited in this text.***

layers of protection against unauthorized attempts by hackers or malicious actors.

4) Keep performance in mind: Performance is critical when providing a great user experience on any digital platform; poor performance leads to poor usability, which can n reduce customer satisfaction levels over time if not addressed quickly enough. It is crucial essential performance in mind while designing applications as this will ensure that they remain responsive even under heavy load times or network delays due to peak traffic periods or the geographic location of customers using your product/service etc.

5) Utilize analytics tools for testing & optimization: Analytics tools are essential for measuring how well users interact with your product/service over time; these insights can then be used to improve design decisions based upon customer feedback, helping shape future releases towards better customer experiences overall!

8 Cyber security and Pakistan

Pakistan is vulnerable to cyber-attacks as its infrastructure and security systems need more resources, personnel, and technology resources against cyber-attacks, making it an attractive target for hackers. Pakistan's economy also suffers from the lack of enforcement of laws related to cyber security. Cybercrime legislation is badly needed in Pakistan, but the government has yet to pass any significant laws that would better protect citizens against attacks. In addition, numerous cybercrimes such as fraud, identity theft, illegal downloads, and hacking remain unresolved due to a lack of resources dedicated to fighting these crimes [25].

For Pakistan to be better protected from cyber threats, it must strengthen its legal framework on cyber security and increase investment into technological solutions that can defend networks from attack. The government needs more effective coordination between law enforcement agencies and tech companies to identify malicious actors online and take appropriate action against them. Additionally, organizations need to promote a more robust culture of cyber security by providing proper training on security protocols so that potential breaches can be identified before they cause severe damage or loss. Furthermore, public campaigns should be conducted nationwide to educate users about what actions to take when using the internet to minimize their risk of exposure to cyber threats [1].

Pakistan's cyber security is a significant concern due to its weak infrastructure, limited resources, and lack of expertise. The Cyber preparedness, elements, and strategic areas are shown in Figure 6. The country is vulnerable to various cyber threats, including data theft or manipulation, ransomware attacks, website defacement, distributed denial-of-service (DDoS) attacks, keylogging, and phishing. Pakistan's legal framework for cybercrime prevention and response is also inadequate due to its lack of expertise in this area. In addition, there is a lack of public awareness of the importance of cyber security and limited resources allocated for developing and implementing effective cyber security measures. Furthermore, government agencies have failed to provide contractors with relevant security training so that they can adequately protect sensitive information stored within their systems. These vulnerabilities are further compounded by the fact that

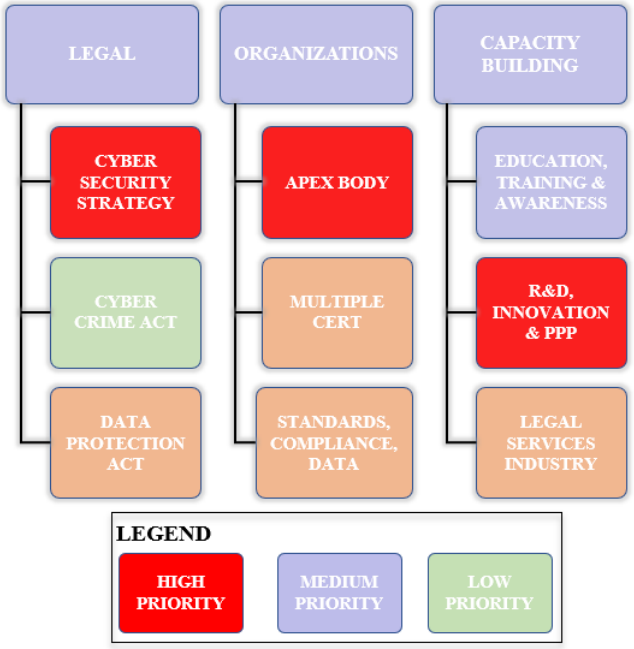

Figure 6: Cyber preparedness, strategic trust areas, and elements

Pakistan has one of the lowest internet penetration rates in Asia, with only 37 million internet users out of its estimated population of more than 200 million. This low level makes it difficult for citizens to access vital online services such as banking or health care, which puts them at risk of being targeted by malicious actors who could use these weaknesses to gain access to personal data or inflict damage upon individuals or organizations operating within Pakistan's borders [6].

9 Pakistan's Preparedness for Cyber Threats

Pakistan is actively engaging in initiatives to protect itself from cyber threats. The government has established the National Cyber Security Authority (NCSA). It is developing comprehensive strategies, policies, and procedures for protecting the country from cyber-attacks [12]. The NCSA also works with various stakeholders, including industry groups, universities, law enforcement agencies, and even other countries, to develop a holistic approach to tackling the issue of cyber security in Pakistan as shown in Table 2. It has put together an extensive policy framework that guides how to deal with incidents of cybercrime as well as directives on how the public sector should respond. Moreover, law enforcement agencies like the Federal Investigation Agency (FIA), the Ministry of Interior's National Response Centre for Cybercrime (NR3C), and the Ministry of Information Technology & Telecommunications' Cyber Crime Reporting Portal are also playing their part in providing quick response to incidents related to cyber security [2].

To ensure an effective response against malicious online activities, Pakistan Telecommunication Authority (PTA) has blocked more than 800 websites hosting anti-state content since 2016. It has taken further proactive steps like setting up a 24/7 monitoring system for social media websites & networks [20].

The last cyber security ranking is shown in Table 2 for the comparison of different countries. In addition, various educational programs are being conducted throughout the country regarding understanding best practices when dealing with cyber security issues so that people become aware of these issues, which can help reduce risks associated with them in the future.

10 Conclusion and Recommendations

In conclusion, Pakistan's current cyber security state is inadequate and poses a severe risk to national security. Numerous reports have been of government and private network attacks, often with devastating consequences. The National Assembly of Pakistan has passed the Cyber Security Act, 2018, which aims to protect citizens from cybercrime by strengthening the legal framework and providing safeguards against cybercrimes. However, the effectiveness of the law is yet to be seen. The lack of competent personnel and resources within governmental agencies means that many organizations must be equipped to respond effectively to threats or defend against them. Additionally, public awareness about cyber security measures must be raised for citizens and businesses to protect themselves from malicious actors. By developing a culture of preparing for and protecting against future attacks, we can reduce the number and severity of incidents our society suffers in this digital age.

1) Improve Governance & Legislation: The government should create and implement strict cyber security laws and regulations to protect the country's cyberspace from malicious activities. This process should include watching citizens' data, imposing penalties on cybercriminals, and protecting critical infrastructure such as power grids and banking systems.

2) Focus on Network Security: Companies need to increase their security investments and focus on updating their networks with the latest cybersecurity solutions. This strategy will enable them to detect malicious activity quickly and prevent significant data breaches.

3) Train Cyber Security Professionals: Companies and government agencies should focus on training cyber security professionals to deal with the ever-growing number of cyber security threats they face.

Table 2: Countries ranking concerning cyber security

Rank	Country	Score	Percentage of Mobiles Infected with Malware	Financial Malware Attacks (% of Users)	Percentage of Computers Infected with Malware	Percentage of Telnet Attacks by Originating Country (IoT)	Percentage of Attacks by Cryptominers	Best Prepared for Cyberattacks
1	Algeria	55.75	22.88	0.9	32.41	0.01	5.14	0.432
2	Indonesia	54.89	25.02	1.8	24.7	1.51	8.8	0.424
3	Vietnam	52.44	9.62	1.2	21.5	1.73	8.96	0.245
4	Tanzania	51.00	28.03	0.7	14.7	0.04	7.51	0.317
5	Uzbekistan	50.50	10.35	0.5	21.3	0.01	14.23	0.277
6	Bangladesh	47.21	35.91	1.3	19.7	0.38	3.71	0.524
7	Pakistan	47.10	25.08	1.4	14.8	0.4	6.07	0.447

4) Increase Cyber Security Awareness: The government and companies should increase general cyber security awareness among the citizens by running campaigns in schools, universities, and other public places.

5) Collaborate with Cybersecurity Companies: The Pakistani government should collaborate with private cybersecurity companies to develop cutting-edge solutions for protecting cyberspace from malicious activities.

References

[1] S. AlDaajeh, H. Saleous, S. Alrabaee, *et al.*, "The role of national cybersecurity strategies on the improvement of cybersecurity education," *Computers & Security*, vol. 119, pp. 102754, 2022.

[2] A. Ali, A. W. Septyanto, I. Chaudhary, *et al.*, "Applied artificial intelligence as event horizon of cyber security," in *International Conference on Business Analytics for Technology and Security (ICBATS'22)*, IEEE, pp. 1-7, 2022.

[3] H. Almarabeh, A. Sulieman, "The impact of cyber threats on social networking sites," *International Journal of Advanced Research in Computer Science*, vol. 10, no. 2, 2019.

[4] J. H. Awan, S. Memon, M. H. Shah, *et al.*, "Security of eGovernment services and challenges in Pakistan," in *SAI Computing Conference (SAI'16)*, IEEE, pp. 1082-1085, 2016.

[5] E. W. Baker, "A model for the impact of cybersecurity infrastructure on economic development in emerging economies: evaluating the contrasting cases of India and Pakistan," *Information Technology for Development*, vol. 20, no. 2, pp. 122-139, 2014.

[6] A. Corallo, M. Lazoi, M. Lezzi, *et al.*, "Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review," *Computers in Industry*, vol. 137, pp. 103614, 2022.

[7] S. Farid, M. Alam, G. Qaiser, A. Ul Haq, J. A. Itmazi, "Security threats and measures in E-learning in Pakistan: A review," *Technical Journal, University of Engineering and Technology (UET) Taxila, Pakistan*, vol. 22, no. 3, pp. 98-107, 2017.

[8] A. Farooq, S. R. U. Kakakhel, "Information security awareness: Comparing perceptions and training preferences," in *2nd National Conference on Information Assurance (NCIA'13)*, IEEE, pp. 53-57, 2013.

[9] M. A. Firdous, "Formulation of Pakistan's cyber security policy," *CISS Insight Journal*, vol. 6, no. 1, pp. 70-94, 2018.

[10] Z. Hussain, D. Das, Z. A. Bhutto, *et al.*, "E-banking challenges in Pakistan: an empirical study," *Journal of Computer and Communications*, vol. 5, no. 2, pp. 1-6, 2017.

[11] A. Khan, M. Ibrahim, A. Hussain, "An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries," *International Journal of Information Management Data Insights*, vol. 1, no. 2, pp. 100015, 2021.

[12] M. F. Khan, A. Raza, N. Naseer, "Cyber security and challenges faced by Pakistan," *Pakistan Journal of International Affairs*, vol. 4, no. 4, 2021.

[13] M. I. Khan, "Cyber-warfare: Implications for the national security of Pakistan," *NDU Journal*, vol. 117-132, 2019.

[14] S. Khattak, S. Jan, I. Ahmad, *et al.*, "An effective security assessment approach for Internet banking services via deep analysis of multimedia data," *Multimedia Systems*, vol. 27, pp. 733-751, 2021.

[15] M. Lyytikinen, P. Yadav, A. T. R. Wibben, *et al.*, "Unruly wives in the household: Toward feminist genealogies for peace research," *Cooperation and Conflict*, vol. 56, no. 1, pp. 3-25, 2021.

[16] Z. U. A. Malik, H. M. Xing, S. Malik, *et al.*, "Cyber security situation in Pakistan: A critical analysis," *PalArch's Journal of Archaeology of Egypt/Egyptology*, vol. 19, no. 1, pp. 23-32, 2022.

[17] A. Naha, "Emerging cyber security threats: India's concerns and options," *International Journal of Politics and Security*, vol. 4, no. 1, pp. 170-200, 2022.

[18] D. R. Naseer, D. M. Amin, "Cyber-threats to strategic networks: Challenges for Pakistan's security," *South Asian Studies*, vol. 33, no. 1, 2020.

[19] S. Rasool, "Cyber security threat in Pakistan: Causes, challenges and way forward," *International Scientific Online Journal*, vol. 12, pp. 21-34, 2015.

[20] K. Shaukat, T. M. Alam, I. A. Hameed, *et al.*, "A review on security challenges in internet of things (IoT)," in *26th International Conference on Automation and Computing (ICAC'21)*, IEEE, pp. 1-6, 2021.

[21] K. Shaukat, S. Luo, V. Varadharajan, *et al.*, "Performance comparison and current challenges of using machine learning techniques in cybersecurity," *Energies*, vol. 13, no. 10, pp. 2509, 2020.

[22] J. R. Sun, M. S. Hwang, "A new investigation approach for tracing source IP in DDoS attack from proxy server", in *Intelligent Systems and Applications*, pp. 850-857, 2015.

[23] J. R. Sun, M. L. Shih, M. S. Hwang, "A survey of digital evidences forensic and cybercrime investigation procedure", *International Journal of Network Security*, vol. 17, no. 5, pp. 497-509, 2015.

[24] J. R. Sun, M. L. Shih, M. S. Hwang, "Cases study and analysis of the court judgement of cybercrimes in Taiwan", *International Journal of Law, Crime and Justice*, vol. 43, no. 4, pp. 412-423, 2015.

[25] F. Z. Syed, S. Javed, "Deterrence: A security strategy against non traditional security threats to Pakistan," *International Journal of Social Sciences and Management*, vol. 4, no. 4, pp. 267-274, 2017.

Biography

Muhammad Ibrar biography. Muhammad Ibrar is with the Software College, Shenyang Normal University. His major is computer science, information secure.

Hang Li biography. Prof. Hang Li is with the Software College, Shenyang Normal University. His major is computer science, image processing.

Jiachi Wang biography. Jiachi Wang is with the Software College, Shenyang Normal University. His major is computer science, image processing.

Shahid Karim biography. Shahid Karim is with the Research & Development Institute of Northwestern Polytechnical University in Shenzhen.