Analyzing cyber-attacks targeted on the Banks of Pakistan and their Solutions

Tanvir Fatima Naik Bukht[1], Muhammad Ahsan Raza[2], Jawad Hussain Awan[3], Rizwan Ahmad[4]
fatimaishtiaq7@gmail.com1 ahsanraza@bzu.edu.pk[2] awanjawadhussain@gmail.com[3] Rk640841@gmail.com[4]
Institute of Southern Punjab Multan, Pakistan[1]
Bahauddin Zakariya University, Multan, Pakistan[2]
University of Sindh Jamshoro, Pakistan[3]
Riphah International University Lahore, Pakistan[4]

Abstract
The main purpose of this study is to analyses the targeted cyber-attacks of Pakistani banks that happened or targeted in 2018 and the solution to control the crimes. The aim of the study is to obtain further information on the impact of cybercrime on the Pakistani banking sector. This study examines the important contribution that raising awareness of the security of information about the relationship between cybercrime and organised services can make. The impact of cybercrime on the Organization's activities will be examined by deepening the moderating effects of raising awareness of cyber security. Cybercrime has a undesirable impact on the organization's performance, but knowledge of cyber security weakens the negative impact of cybercrime on the organization's performance. This study focuses on the banking sector and therefore cannot be extended to other sectors. In addition, comprehensive relative studies in other areas with different cultural contexts will contribute to the validation of the research results. Awareness about the security of information weakens the negative effect of cybercrime on performance; therefore, it is important for banks, security, human resource supervisors, training to raise awareness of employees about cybercrime. Cyber-attacks, threats, vulnerabilities, Security attacks and challenges combination of these topics has led to a new study in the field of cybercrime. This study also improves the understanding of the role of employees in combating the effect of cybercrime on organizational performance.

Key words:
Analyzing cyber-attacks, attack targeted on the Banks, attack on Pakistan's bank, cyber-attacks.

1. Introduction

The increasing number of cyber-attacks on digital technology and communication networks attracted the attention of ICT professionals, cyber security wings and other security officials to enhance the security level. Now, cyber-attacks have turned out even more complex and improved[1]. Generally, our society, and economic system and the critical infrastructures are depending largely on information networks and IT solutions. Hence, their security has a big concern. In addition, a cybercrime and security survey report recognized that injecting malware, phishing, computer theft and bot attacks are common approaches to cyber-attacks to attain sensitive material and thus cause damage to organizations[2].

Mobile banking is one of the latest improvements in the banking sector. This means that customers and banks communicate online. Peoples/ clients now choose Online facilities because they are more suitable, inexpensive and easier and quicker to use. There was also the introduced of mobile money transfer via mobile networks and in Pakistan via services such as MobiCash and Easypaisa. Therefore, banking services has made accessible to many people using technology by improving user-friendliness and availability. Mobile banking sector despite the advantages, it has been found that many applications based on Smartphones are not security-oriented and often do not comply with best practices.

This research paper is ordered as follows. Section 2 defines an overview of the importance of cybersecurity. Section3 express information related Cyber-attacks, threats, vulnerabilities, and strategies. Security attacks discussed in Section 4 and Section Analysis of Pakistani Banks targeted by cyber-attacks in 2018. Section 6 describes vulnerable cyber-attacks and threats and their solution and listed the solution to control the crimes, also include solutions to cope with cyber-attacks, threats, vulnerabilities and the basic components of technological and tactical.

2. Importance of Cyber Security

Due to the development of ICT and cyberage, various number of privacy and security challenges have been identified and reported. Hence, a new field is extended in cyber world titles as Cyber security. Thus, a question arises "Why Is Cyber security Important?" The answer to that question is answered. It has importance because of the emergence and progress in the field of ICT has played a vital role. Therefore, privacy and information security are always the most important security features of a business. We are in a global location where all data stored in a digital or cybernetic format. Social networks offer a space in which users can comfortable with friends and family. For

Manuscript received Fabruary 5, 2020
Manuscript revised Fabruary 20, 2020

domestic employers, cybercriminals would remain to visit social networks to snip private information. But not only in social networks does a person have to take all necessary security measures in banking transactions[3]. Basic frameworks of government, organizations, military, money related foundations, emergency clinics and different organizations are rehearsing security forms, devices to keep up the expanding level and entanglement of digital assaults and ensure private data put away in databases, systems and servers[4][5]. There are too many threads such as content-related, the Trojan House, Spam, Frauds, Phishing, Cyber Harassment, Intrusion, Malicious code, Denial of services, APTs (Advance Persistent Threats), Zero-day attack, etc[6]. We can secure our data by using cyber security techniques such as security password, data of authentication, software anti-virus, firewalls and scanners for malware [7]-[8].

3. Cyber-attacks, threats, vulnerabilities, and strategies to cope with them

When we think about information technology / cyber security, the 1st thing that strikes me is "cybercrime", which is gradually increasing. Illegal activity in term of Cybercrime which a computer is used as a primary means of education and theft. In general, cybercrime is definite as a crime committed through the using a computer and the Internet to steal a person's identity, to track down victims and information. As step-by-step technology plays an important role in a person's life, cybercrime will growth with technological advantages[3]. Traditional malware attacks occurred at a single point on the surface between hardware equipment, software sections, and network layer, using the existing project incorrectly[9]. Cyber-attacks are direct attacks through cyberspace to an organization that uses the Internet through the disorder, destruction, deactivation and malicious control of the organization's IT infrastructure[2]. Knowledge of cyber Security has a positive effect on the working of the organization[10].

Computer security is a big challenge for many countries. It is accepted that cyber terrorists become too smart and able to create attacks of confidentiality, availability, and integrity in various information technology services such as government database services. Security, flexibility and consistency of IT resources and government services in the nation are another major challenge for management and as a growing number of attacks is a threat to national security that causes financial loss or more serious data[11]. According to approximations[12], by 2020, 38.5 billion devices are connected to the Internet to generate and disseminate confidential information worldwide. In this Situation, two new challenges arise, such as unrelated data and a large number of events are identified. Heterogeneous data is data that modified from the type of device and uses standardized rules but also different protocols for the exchange of information. While a large amount of event is a multitude of facts and actions flow into data and communication systems.

4. Security attacks

Attack is any cybercriminal action, try to access confidential data the security of facts owned via an organization using any system that designed to detect[13]. Cyber-attacks from different perceptions are critical in order to moderate them[14]. There are several forms of attacks; however, the most commonplace security attacks are described.

4.1 Denial of Service attacks

These attacks are specifically used to disregard certain resources, such as an Internet server for users. These attacks are very common today[15]-[16].

4.2 Brute-force attacks

It is a challenge for trial and error to guess the password of a system. Every fourth network attack is an attempt to brute force. In this attack, computer software was used to provide hundreds or thousands of password combinations[15]-[17]-[18].

4.3 Browser attacks

Browser attacks targeted at customers surfing the Internet. Attacks can also encourage them to download malware without realizing it. These attacks used fake software to replace, update, or apply. Websites are also needed to download malware. High-quality approaches are to avoid full browser-based network attacks to update web browsers frequently[15].

4.4 Shellshock attacks

Shellshock attacks address the vulnerabilities in Bash, a collective command-line shell for Linux and UNIX systems. Because many installations are never updated, the vulnerabilities still exist on the Web. The problem is that Shellshock is the target of all networks[15].

4.5 Distributed Denial of Service

The interruption of external procedures is done through a DDOS (Distributed Denial of Service) attack or damage to the website. The external overflow of requests to an Internet site server is also a familiar type of interruption event, has the potential required and devastating [19]. For example, a large commercial furniture manufacturing company whose site purchase website will not be displayed for 20 hours, while this type of event may also create a problem in the online shop based store[20]-[18].

4.6 Secure Sockets Layer (SSL) attack

These attacks are intercepted information sent over an encrypted connection. These attacks effectively access information without encryption. One of the most common attacks today[15]. The disruption of the internal processes is also performed by an internal multi-point elimination, which manages user data, encryption and eradication of the main systems[20]-[9].

4.7 Backdoor attacks

Backdoor attacks are used to prevent common authentication for remote access. These attacks are added to the software program using the theme. These are added to the programs or created using a current program. The rear doors are not so common[15].

4.8 Botnet attacks

Botnet attacks are thieves. One or more malicious actors are remotely controlling the information systems. Attackers use botnets for malicious activity or engage bot-nets to perform activities that are harmful to others. When acquiring a bot-net, millions of computer systems can be repaired[15].

4.9 Message manipulation

The attacker tries to hijack the user's personal data, information, social media and website accounts. The hacking of user accounts is insignificant only in social networks, customer accounts that are not directed with their computers. For this reason, these interruption activities have negligible coverage compared to other interruption events[20].

4.10 Interruption of internal communication

The interruption of internal operations takes place through the Denial of Service (DoS) of a network. In rare cases, this type of interruption may take time to fully recover in days, weeks and months[20].

4.11 Information attack

An advanced controls the disposition of a network to transfer the malicious code between the network of connected computers to alter, at the same time it corrupts the operating systems of computers, deletes the files, regulates the firmware and attempts to destroy the peripherals[20].

4.12 Hardware/ Tool Attack

The unauthorized access right has a network to destroy a physical system between the digital and the physical world, as well as highlighting an exposure to the critical system that can preserve current life. This type of criminal activity requires a deep knowledge of the system and its network with essential resources and management structures[20] as shown in Figure 1.

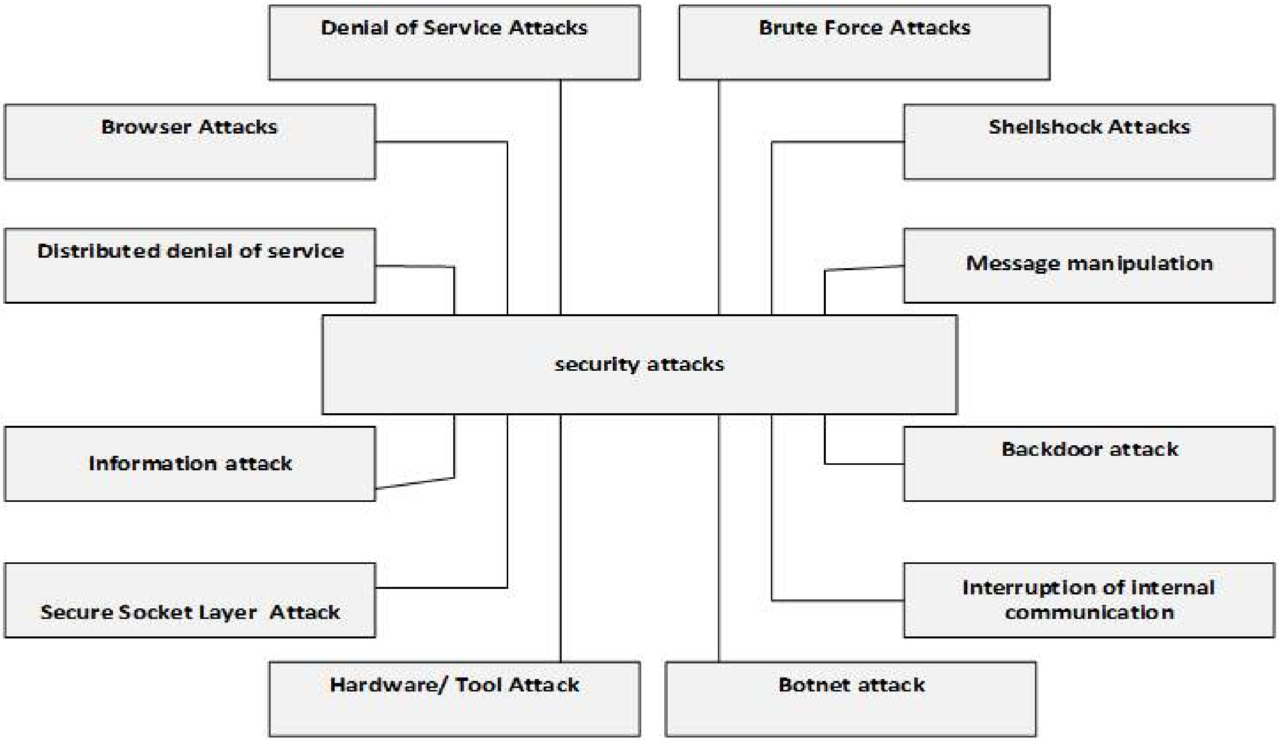

Fig. 1 Show the most common security attacks

5. Analysis of Pakistani Banks targeted by cyber-attacks in 2018

The information and data on 19,864 cards, which are among the customers of 22 Pakistani banks, give the dark side a signal, as a study by the Pakistan Computer Emergency Response Team, PakCERT, shows. It all started in mid-October 2018 when some of Islami Bank's clients received text messages warning them against a cash exchange, which they did not. In an irregular trade amounting to Rs 2.6 million (US $ 18584.70), Islami Bank blocked its international payment plan on October 27, 2018. Hackers carried out these international ATM transactions with cards issued by the bank. In fact, when PakCERT investigated the cyberattack, it found that information about 20,000 debit cards was negotiated. In addition, it can clarify the news that some of you have received from their banks, who have recently reported that the card has been blocked for international transactions, for safety reasons[21]-[22].

On October 26, 2018, a copy of the data and information with over 9,000 debit cards was published in the dark network. When everyone thought the storm was greater than October 31, 2018, a second landfill of over 12,000 Darknet cards was issued, including 11,000 cards from Pakistani banks. The Islamic Bank was the main bank that went public, but the report said that a large number of control cards from 21 different banks were available for purchase in the dark web. The Dark Web is known as a hotbed of criminal movement and cannot be restored without Tor software, an anonymous communication.

The news came after a cyber-attack on the Islami Bank of Pakistan a week earlier, taking at least $ 20,000 out of their accounts[22]. The cost of the deal for these cards has increased from $ 100 to $ 160 (from RS 13990 to 22384.00). Of all banks, HBL, the largest bank in the country, was the most notoriously affected by over 8,000 cards, followed by UBL, Standard Chartered Bank, MCB and Meezan Bank, each with over 1,000 cards.

Alfalah Bank, Islami Bank and the Bank of Punjab were among the banks that saw over 500 of their cards thrown into the dull network or web. As stated by PakCERT, the pirated copies of credit card information can be accessed in two configurations. First, credits such as full name, address, phone number, card number, and expiration date can be easily used by someone for illegal online purchases. The second configuration is represented by the scanned dumps. This means that the hacker was physically willing to check and scan the details of the card at an ATM or a compromised commercial computer or trade machine for illegal trade.

In addition to the Pakistani customer data, maps of non-Pakistan banks such as Emirates Nbd, Abu Dhabi Islamic Bank, Citibank USA, National Bank of Abu Dhabi and the Commonwealth Bank of Australia were discarded Visitor data He traveled to Pakistan at that time and used one of the ATMs or cooperative commercial machines[21].

The State Bank of Pakistan (SBP) said that banks themselves were not hacked. "It has been noted with concern news things detailing that the information of most banks has been hacked. SBP completely rejects such reports,"[22] an announcement from the national bank said. This is additionally supported by a report by Pakistan Computer Emergency Response Team (PakCERT) which details out the timeline and scale of data leaks. It supported the SBP's claim and said that the information was no doubt spilled through card scanning. Card skimmers are devices that can be used to copy and collect the details enclosed in a credit card's magnetic stripe they came into exchange with. Using this wrongfully found data, Hackers can conduct credit card frauds[23] as shown in Figure 2.

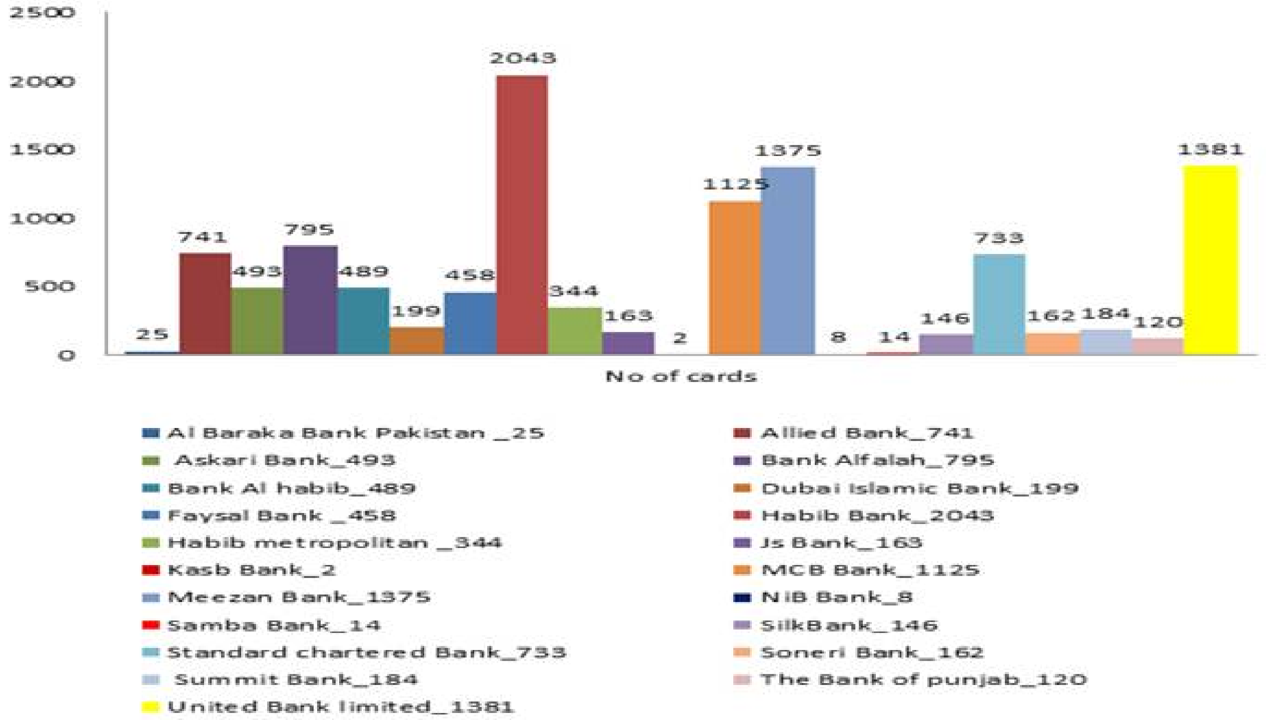

Fig. 2 Banks and number of cards attacked

6. Vulnerable Cyber-attacks and Threats and their Solution

Whenever we think about cybersecurity, the first thing that comes to mind is "cybercrimes or cyber-attacks", which increase gradually. Cybercrime is a term for any illegal activity that uses a computer as the primary means of education and theft. In general, cybercrime can be defined as a crime committed by using a computer and the Internet to steal a person's identity, track down victims and information. As step-by-step technology plays an important role in a person's life, cybercrime will increase with technological advantages[3]. Traditional malware attacks occurred at a single point on the surface between hardware equipment, software sections and network layer, using the existing project incorrectly[9]. Cyber-attacks are direct attacks through cyberspace to an organization that uses the Internet through the disorder, destruction, deactivation and malicious control of the organization's IT infrastructure[2]. According to approximations[12], by 2020, 38.5 billion devices will be connected to the Internet to generate and distribute sensitive information around the world. In this condition

6.1 Main challenges

Bank sector all over the world are facing the most common two factors. First, heterogeneous data where modified device use standardized and different protocols for communication purpose. Second, the large number of events where a multitude of information and events flow into data and communication systems. A delegation from Tanzania recommends that Pakistan set up the Cybercrime Unit (CCU) to commit cybercrime, develop a standard and formulate an emergency computer response group (CERT) to facilitate its implementation. Tanzania has lost $ 6 million on numerous cybercrime forced to develop CCUs and CERTs.

The dignitaries of the task said they lost $ 445 billion a year in cybercrime and automatic theft of online security services. In addition, 800 million documents from developing countries are forged. In this context, developing countries such as Pakistan should recommend, together with industrialized countries, a strategy to combat crime[5]. To save the lives of innocent people, we recommend creating proper directions for the virtual world according to real life. Additionally, new security actions are needed to defend privacy in the virtual world[24]. Other countries like the United States UU. This is an important step in communication and IT. Countries use a variety of tools, mainly electronic observation platforms, terrestrial intelligence and aircraft such as call recording, stage satellites that can collect impulses. Open the message by filtering e-mails. Leakage, radio monitoring, IT-based vulnerability in networks that either secretly or openly transport sensitive data and other sophisticated media[25].

6.2 Recommended Solutions to cope cyber-attacks, threats, and vulnerabilities

The definition above can be as intellectual as a cybernetic defense cycle containing four components, namely prevention, detection, and forensic reaction. Prevention, detection, reaction and forensic are four basic techniques to identify, cope and deal with them. Further discussion as under and Table 1:-

Table 1: Solutions to manage cyber-attacks, phase detail

SNo	Method / Phases	Details
1	**Prevention**	Prevention is better than cure. It's better to avoid an attack before it takes place. High-quality security software needs to be installed on your computers to report your work and your private virus data.
2	**Detection**	Detection can identify security incidents. It is also used to monitor and redirect network traffic to protect a System.
3	**Reaction**	Reaction happened when cyber-attack successfully happened, it has to be quickly clarified whether and to whom the accident has to be reported. This obligation may be primarily due to the data protection act13.
4	**Forensics**	When an attack is eliminated and the System heals, this Phase is used13.

1. The prevention section is responsible for constantly monitoring the device in order to detect any vulnerability or incorrect configuration within.
2. The detection section is the use of IDS such as Network IDS, Host base IDS, Signature-based IDS, and Anomaly based IDS. We can use Wireshark to detect traffic (good or bad traffic) in our server, which is also helpful for us to know about the attacker.
3. The reaction phase is used to provide quick remove the attack.
4. When an attack removed and system heals then the forensic phase is used[12].

In addition, the basic components of technological and tactical solution are as follows:-

1. The physical system (Monitored system) is used to protect the system, central monitoring information, including the topology and configuration of network assets[26]
2. Number of instruments (like detection tools) that send all events occurring in the control system. These occasions consist of intrusion signals, software updates, hardware installations, etc. Some examples of this device are IDS, Antivirus (AV), and FW.
3. Countermeasures for acknowledgment of receipt such as closing TCP / UDP ports, redirecting incoming traffic, applying a route, etc.
4. Measure or monitor vulnerability response also characterizes information on vulnerabilities.
5. System modal assumes that the information collected by the supervised system, such as the network topology.
6. Atomic technical solution is data that has not been prepared and converted into corrective actions will identify the knowledge of countermeasures, a list of promising countermeasures will be generated, and an attempt will be made to combine the above remedies to prevent the attacks.
7. Thread model is based on vulnerability checks and the system model, a threat model representing attack models was created
8. In Select action, some countermeasures are selected by balancing the exchange between the safety phase of the machine and the cost of the reaction. In particular, this problem is not simply a matter of the monetary value of activating the selected movements, but also of the potential negative effect of compliance, the possible reduction in the availability of one or more services. Analyze and classify a set of possible countermeasures for a selected attack and try to maximize their value, effectiveness, limit, or cost[12].
9. To protect data it is also important to use secured and advanced software for detection of attack. We can also use Wireshark for detection of attacker

the source IP address. In this way, we can protect our data by block incoming viruses and attack.

7. Conclusion

Cybersecurity is a global field, designed to protect and monitor networks, computers, data and programs from unauthorized access or misuse. The most important task of a cyber-security analyst is to protect a network from damage. In this study, we express information related cyber-attacks, threats, main challenges and also provide some solution to control the crime, some cyber security attacks and defines strategies to overcome cyber-attacks. In addition, we introduce and discuss cyber security and its importance. Moreover, it analyses information related security, cybercrime and cyber-attacks. This study also analyses the targeted cyber-attacks of Pakistani banks, happened or targeted in 2018.

8. Future Work

Pakistan is the future and improving state of South Asia day by day. Even, the government is trying to develop such policies to integrate security measures to enhance the capabilities of existing systems to prevent future cyber targets. In this way, the opportunities for the security of banks, critical infrastructure and major sectors are under consideration and needs more research in the security and privacy of such deployed systems of Pakistan.

References

[1] W. Meng, E. Tischhauser, Q. Wang, Y. Wang, and J. Han, “When Intrusion Detection Meets Blockchain Technology: A Review,” IEEE Access, vol. 3536, no. c, pp. 1–10, 2018.

[2] J. Omidosu and J. Ophoff, “A theory-based review of information security behavior in the organization and home context,” Proc. - 2016 3rd Int. Conf. Adv. Comput. Commun. Eng. ICACCE 2016, pp. 225–231, 2017.

[3] G. N. Reddy and G. J. U. Reddy, “A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies,” p. 5, 2014.

[4] J. H. Awan, S. Memon, S. M. Pathan, M. Usman, and R. A. Khan, “A user friendly security framework for the protection of confidential information A user friendly security framework for the protection of confidential information,” IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 17, no. 04, pp. 215–223, 2017.

[5] J. H. Awan, S. Memon, M. Shah, and F. H. Awan, “Security of eGovernment Services and Challenges in Pakistan,” in SAI Computing, 2016, pp. 1082–1085.

[6] J. Awan and S. Memon, “Threats of Cyber Security and Challenges for Pakistan,” in 11th International Conference on Cyber Warfare and Security: ICCWS - 2016, Boston USA, 2016, p. 425.

[7] S. A. Memon and J. H. Awan, “Transformation towards Cyber Democracy: A study on Contemporary Policies, Practices and Adoption Challenges for Pakistan,” in Handbook of Cyber-Development, Cyber-Democracy and Cyber-Defense, 2017, pp. 1–20.

[8] E. M. O. Abu-Taieh, “Cyber Security Body of Knowledge,” 2017 IEEE 7th Int. Symp. Cloud Serv. Comput., pp. 104–111, 2017.

[9] J. Jang-Jaccard and S. Nepal, “A survey of emerging threats in cybersecurity,” J. Comput. Syst. Sci., vol. 80, no. 5, pp. 973–993, 2014.

[10] M. S. Malik and U. Islam, “Cybercrime: an emerging threat to the banking sector of Pakistan,” J. Financ. Crime, vol. 26, no. 1, pp. 50–60, 2019.

[11] 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 Warf. Terror., vol. 9, no. 2, pp. 29–38, 2019.

[12] P. Nespoli, D. Papamartzivanos, F. G. Marmol, and G. Kambourakis, “Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks,” IEEE Commun. Surv. Tutorials, no. c, 2017.

[13] N. Ben-Asher and C. Gonzalez, “Effects of cyber security knowledge on attack detection,” Comput. Human Behav., vol. 48, pp. 51–61, 2015.

[14] F. Chowdhury and M. S. Ferdous, “Modelling Cyber Attacks,” Int. J. Netw. Secur. Its Appl., vol. 9, no. 4, pp. 13–31, 2017.

[15] P. R. P. Jitendra Jain, “A Recent Study over Cyber Security and its Elements,” Int. J. Adv. Res. Comput. Sci., vol. 8, no. 3, pp. 2015–2017, 2017.

[16] M. AAMIR and M. A. ZAIDI, “A Survey on DDoS Attack and Defense Strategies: From Traditional Schemes to Current Techniques,” Interdiscip. Inf. Sci., vol. 19, no. 2, pp. 173–200, 2013.

[17] R. M. Yousufi and P. Lalwani, “A Network-Based Intrusion Detection and Prevention System with Multi-Mode Counteractions,” 2017.

[18] L. Liu, O. De Vel, Q. L. Han, J. Zhang, and Y. Xiang, “Detecting and Preventing Cyber Insider Threats: A Survey,” IEEE Commun. Surv. Tutorials, no. c, pp. 1–21, 2018.

[19] J. H. Awan, U. Naseem, and S. K. Khan, “A proposed farmework for the security of Financial Systems,” Indian J. Sci. Technol., vol. 12, no. 21, 2019.

[20] J. H. Awan, S. Memon, R. A. Khan, A. Q. Noonari, Z. Hussain, and M. Usman, “Security strategies to overcome cyber measures, factors and barriers,” Eng. Sci. Technol. Int. Res. J, vol. 1, no. 1, pp. 51–58, 2017.

[21] J. H. Awan, S. Memon, S. Memon, K. T. A. J. Pathan, and N. H. Arijo, “Cyber Threats/Attacks and a Defensive Model to Mitigate Cyber Activities,” Mehran Univ. Res. J. Eng. Technol., vol. 37, no. 2, pp. 359–366, 2018.

[22] F. Baloch and I. Firdous, “Pakistani banks hit by biggest cyber attack in country’s history,” Samaa Web, 2018. [Online]. Available: https://www.samaa.tv/news/2018/11/pakistani-banks-hit-by-biggest-cyber-attack-in-countrys-history/. [Accessed: 25-Jan-2019].

[23] Almost all Pakistani Banks’ Data Has Been Breached, And For Sale On The Dark Web | Page 7 | Eyerys.” .

[24] 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, pp. 1–8, 2019.

[25] J. Raiyn, "A survey of cyber attack detection strategies," Int. J. Secur. its Appl., vol. 8, no. 1, pp. 247–256, 2014.

[26] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," IET Cyber-Physical Syst. Theory Appl., vol. 1, no. 1, pp. 13–27, 2016.

Ms. Tanvir Fatima Naik Bukht is a research student at the Institute of Southern Punjab Multan, Pakistan. Her research interests are Cyber Security, Information Security, digital image processing, IoT and Security challenges in Information Systems. She did her Masters in Computer Science (MCS) from the Virtual University of Pakistan and now studying MPhil from Institute of Southern Punjab Multan, Pakistan

Muhammad Ahsan Raza holds a PhD degree in Computer Science at the Department of Computer Systems & Software Engineering, University Malaysia Pahang, Kuantan, Malaysia. His main research interests include semantics, computer networks and computer security

Dr. Jawad Hussain Awan is a member of IFIP WG 9.10 - ICT Uses in Peace and War, active researcher of Global Foundation for Cyber Studies and Research Group. He is Research Fellow, at Institute of Information and Communication Technology, University of Sindh, Jamshoro, Pakistan. His research interests are Cyber security, Information Security, e-Governance, e-Democracy, Security challenges in Information Systems and Smart Systems. He published his research in several national and international research journals. Dr. Awan attended and presented his research in national and international conferences. He the member of Editorial Review Board of International Journal of Cyber Warfare and Terrorism Journal, International Journal of Digital Cyber Forensic, Egyptian Journal of Informatics, and Cyber Policy. He is also Microsoft Certified Professional in Web Programming. He also worked as Lab Manager, Lecturer and Research Fellow

Mr. Rizwan Ahmad is a research student at Riphah International University, Lahore Pakistan. His research interests are Cyber Security, Network Security, Information Security and ICT. He received his B.Sc degree from Bahauddin Zakariya University Multan, MCS degree from Virtual University of Pakistan and now studying MSCS from Riphah International University Lahore Pakistan