ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 12(21), DOI: 10.17485/ijst/2019/v12i21/143891, June 2019*

A Proposed Framework for the Security of Financial Systems

Jawad Hussain Awan[1], Usman Naseem[2] and Shah Khalid Khan[3]

[1]Institute of Information and Communication Technology,University of Sindh, Jamshoro, Pakistan; awanjawadhussain@gmail.com
[2]University of Technology Sydney, Sydney, Australia; usman.naseem@student.uts.edu.au
[3]RMIT University, Melbourne, Australia; shah.khalid.khan@rmit.edu.au

Abstract

Objectives: This study proposes a framework for the enhancement the security level of the eBanking or online banking systems. **Methods/Statistical Analysis**: Financial system has been categorically considered as a major critical infrastructure of community, society and country. In addition, the constantly rising number of breaching attacks increased and targeted via Internet. It is therefore recommended to provide more security to such systems from malicious activities. In this regard, this study overviews comprehensive highlighted security challenges, security attacks. In addition, a security framework is also proposed to enhance the security level of discussed systems. **Findings:** The proposed framework of the system is categorized into two: The first one category discusses Network Standards for the Security of System and the second category is based on architecture of the system. In Network Standards for the Security of System, two standards are defined, one for wired connection while others for wireless connections. The second part is most significant section of the paper, which is comprised of three stages. Stage one comprises basic Security requirements, Stage two defines parameters of Wireless Security design and the third stage deploy security algorithms and techniques to offer secure network. Availability, Reliability, Authentication, Access Control, Information and Message Confidentiality, Information and Message Integrity, Reliable Message Delivery, Non-repudiation are basic requirements are basic requirements. Authentication, Authorization, Secrecy Capacity, Intercept Probability, Complexity, Encryption and Latency are major parameters while Theoretic security, Security diversity methods, Artificial Noise aided security, Physical layer secret key generation and Security oriented beam forming are defined algorithms in this study. **Application/Improvements:** The proposed framework includes two major parts. First part is about enhanced Network Standards for the Security of System while second part illustrates architecture of the proposed framework.

Keywords: Algorithms**,** Financial System, Framework, Network Standards, Security

1. Introduction

The development and invention of Chip technology is becoming ever more vulnerable to malevolent activities and enhancement with globalization. It has elevated solemn concern about potential intimidation to martial systems, critical infrastructures and home appliances. An adversary can initiate a Trojan malware intended to stop and annihilate the process or functionality of system at various instance or Trojan malware may provide to escape secret information secretly to the opponent[1-3]. The significant rising demands of mitigating victims from cyber event for financial compact have been motivating the speedy growth of the cyber security Insurance.

The accomplishments of Critical Infrastructure (CI) have enclosed a range of phases in cyber incidents, from chopping to frauds. Though, CI is at discovering phase: therefore, current application tools have uncovered some dimensions. The cyber incident on Critical Infrastructure is one of the solemn concerns that prevent the growth of CI. This study also overviews and designed an approach for matching diverse cyber risk scenarios, which utilizes

*Author for correspondence

repository data[4].The cited study[5], identified few primary structure of infrastructure that offered the essential stage of verification and reliability. It also recommended unremitting knowledge and training schemes which are conducted frequently to guarantee that users have know security bullying and identify possible issues and strategies to preserve a protected eGovernment service. Besides, cyber security policies have also discussed recommended and suggested for eGovernment and its services which are very essential for existing security situation in the country to be protected. Pakistan is one of the developing countries, which have set up ICT and online services. From the reports[6], phishing campaign and Dyre banking malware are witnessed, that the stolen information such as user's confidential credentials are forwarded to malicious players. These malware embarked growing cyber issues for developed and developing countries, which regularly target the correspondent, add-on, exploit idea and payload. In[7], a security technical framework has been developed to detect vulnerabilities Such as: XSS attack, session riding and more. This developed framework also implemented superior detection and fuzzing technology to detect vulnerabilities and increase the security level and identifies possibilities of significant databases via scanning process as URL is working which took place that time. So, this research helps, supports and protects the credential information existing or stored in databases. It also detects cyber terrorist activities and their level at monitoring and supervision stages from illegal access or spoil, which is caused by cyber terrorist. In addition, the paper overviews the existing rising problems, obstacles, cyber threats, cyber-attacks and few research directions. However,, current functional systems, their operations, complexities, and services, essential interruptive cyber measure modules are basis strategy for malicious activists to suspend a targeted network.

The categorization of these modules is permit to distinct actions either presented in same class or dissimilar classes[8]. Further, the researchers and technologists proposed two basic goals such as: advanced level knowledge of these issues and their possible solutions. Hence, it is important to take a short preview of the all features existing in a ordered form from the fiscal inspiration and necessities on sharing of information over authorized and rigid feature to structural and industrial theme. Consequently, this study highlights following points as under:

- Holistic representation of Information division.
- Review on presented techniques, ICT tools, Protocols and solutions to discover open gaps.
- Appraisal of the modern and key findings for upcoming Systems.

This study comprises of five sections. Section I is based on Introduction. Section II highlights the work done and background studies as Literature Review, Section III discusses the solution of identified problem. In addition, Section IV discusses and illustrates the proposed framework, which is further categorized into security protocols architecture of framework, and Section V concludes the study with discussion.

2. Literature Survey

The emerging of big data with other fields has increased a wide number of integrity, availability, security and privacy issues[6].

Innovations, emergence, benefits provided to people and users have arose a range of challenges. Hence, the emergence of new technology creates troubles as well like privacy[9]. These days, all the organization like face book, twitter, academia, Google, Gmail have revised their policies to tackle security issues. Even tough, academia and research institutes have also defined their policies[10]. The ongoing research in pervasive computing, IoT, Big data, WSN and other fields have similar issue of security. Therefore, the need of cyber security is increased all over the globe. In addition a question is unanswered yet. "What exactly can be done to resolve confidentially and privacy issues of big data? To get answer of this question, the author cited in[1] has analyzed 58 research articles from 2007 to 2016. As a result, researcher has identified security research gaps, faced by immense companies with modern industrial development in commercial societies and attracts the attention of academicians, researchers and professionals to provide innovative research solution of them[11]. In addition, the technology is emerged with eCommerce to provide efficient and effective user services. Hence, modern transaction and ePayment to online services has encouraged the bank clients to use online or eBanking services. Like other fields and systems, eBanking systems have also security and usability challenges. In this regard, the government and private organization have invested

to improve the performance of banks and transaction systems as well as to deal or overcome privacy issues[12]. In[13], authors have discussed a security and usability evaluation model to assess meticulous privacy and usability features of the systems as well as supports in the development. The authors further added the evaluation framework. At initially level, the identified and compared the previous existing metrics of reviewed literature with modern metrics identified by authors in above cited research paper. In next stage, inspection model is structured to evaluate internal and external usability or security of eBanking systems. In addition, a framework is proposed to enhance the existing security of system. Like National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) lack the privacy and usability features in the performance or best practice for most secure systems[14]. Besides these challenges, online or eBanking is easy and effective practice by clients to use financial services at door step. Unfortunately, the threats and malicious activities towards financial services have reduced the clients' attention to use banking services online[15]. But, the market demands ease of use and security of proposed or developed systems for customers. From the report cited in study[6,16] mentioned that 47% of financial or banking services have been targeted in previous years. In addition, the authors in study[17], highlighted security issues in the banking systems of Malaysia. 137 online participants along with 37 interviewed participants were analyzed in their research to know the reason behind the security of banking. The outcome of the conducted interviews and participants response have suggested that end-users experience major complexity in learning scientific terminologies, privacy features and additional practical concerns or challenges. It represented that the end-users are also incapable to deal with technical concerns at implementation level[18].

3. Problem Statement

From the studies discussed in literature section has notified and identified eBanking and financial systems issues. Security and usability are most of the concerns as well as those are identified by researchers, technical personals in their cited research[19,20]. In addition, it is recommended and suggested to propose a framework for the enhancement the security level of the eBanking or online banking systems. Though, a framework is proposed and illustrated in section IV.

4. Proposed Framework for Financial System

The proposed framework of the system is categorized into two categories as shown in Figure 1. The first one category discusses Network Standards for the Security of System and the second category is based on architecture of the system. Both are discussed as under.

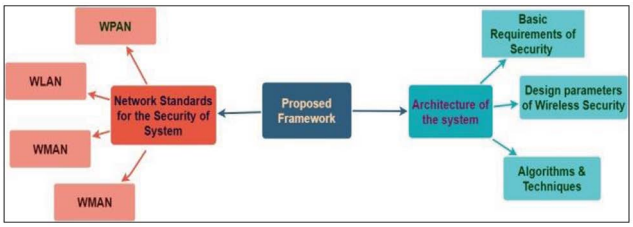

Figure 1. Proposed framework.

4.1 Network Standards for the Security of System

The specified area is centered on the cluster of security conventions and standards that are utilized for enhancing the security of remote systems. When contrasted with wired systems, the remote systems have the upside to maintain a strategic distance from an expensive link based framework, which is sent through this process. Figure 2 illustrates the adapted delineation of operational remote systems, where the collection of Wireless Personal Area Networks (WPAN), Wireless Local Area Networks (WLAN) and Wireless Metropolitan Area Networks (WMAN) are characterized, and furnishes the omnipresent broadband remote administrations to the clients on their demand. The goal of these protocols is to examine the WPAN, WLAN, WMAN and WWAN procedures from alternate points of view, mechanical norms, scope zone and peak information rates. Especially, a WPAN is regularly utilized for connecting with individual gadgets (E.g., a console, sound headphones, printer, and more) at a low information rate and inside scope region.

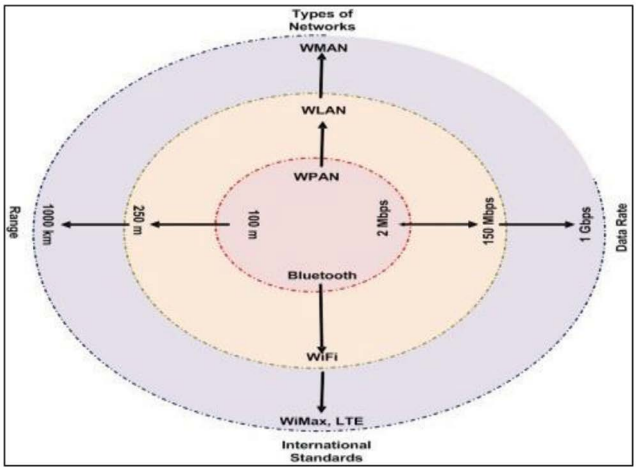

Figure 2. Security defense protocols and paradigms for financial system.

For instance, Bluetooth is a most common and typical wireless standard, mostly used in communication over small space via Ultra High Frequency (UHF) in the band of Industrial, Scientific and Medical (ISM) ranges from 2400 to 2485 MHz with 100m and 2 Mbps from devices, and structures Personal Area Networks. Figure.1 additionally demonstrates that a WLAN has an advanced data rate 1Gbps and 1000 km range, which is greater than the WPAN. It utilized to associate remote gadgets during an Access Point inside a nearby scope area. For an example: IEEE802.11 is a WiFi standard, and comprises of a progression of modern WLAN standard. Presently, Wi-Fi gauges are equipped for a peak 150 Mbps as and 250m of range distance. Metropolitan city is at a higher data rate and over coverage territory other than the Wireless PAN or LAN. For example, in Figure 1, two sorts of modern guidelines for WMAN are highlighted, to be specific Worldwide Interoperability for Microwave Access (WiMAX) and Long Term Evolution (LTE). In the accompanying, we will display an outline of the defense conventions utilized as a part of the previously mentioned remote norms for ensuring the credibility, classification, uprightness, and accessibility of honest to goodness transmissions through the remote spread medium.

4.2 Architecture of Proposed Framework

This section is most important part of the paper, which is comprised of three stages. Stage one comprises basic Security requirements, Stage two defines parameters of Wireless Security design and the last stage deploy security algorithms and techniques as illustrated in Figure 3 and discussed in sub section.

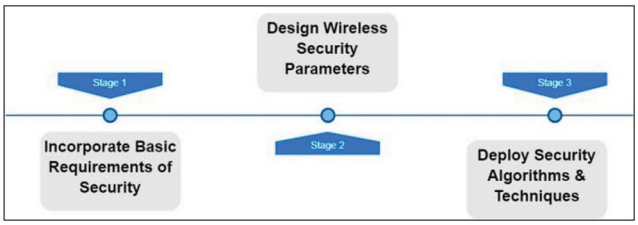

Figure 3. Architecture of proposed framework system

4.2.1 Basic Requirements of Security for Financial Systems

This sub-section defines some security requirements, which are essential for financial systems to provide reliable security. Availability, Reliability, Authentication, Access Control, Information and Message Confidentiality, Information and Message Integrity, Reliable Message Delivery, Non-repudiation are basic requirements shown in Figure 4. Availability represents the ability to use systems, networks and sensitive information for the infrastructure endurance, when the system is working under tremendous situations. Secondly, Reliability is the ability to guarantee that a system or network will execute its anticipated purpose lacking collapse at explicit situations for a particular time gap. Besides this, Authentication is the ability to recognize a client or user that is suitable to the explicit information, service and provide access controls. Access Controls are defined as the ability to guarantee that only approved users can use the system and network assets such as Information and Message Confidentiality. Information and Message Confidentiality guarantee that only approved users or staff used secured information and encrypted messages.

Information and Message Integrity also ensure the information, which is supervised by the systems and non-distorted messages conveyed over the network by illegal users or non-assured software or hardware. Reliable Message Delivery is useful to evade message failure and imitation as well as promise structured liberation along with the capability to mutually offer confirmable evidence of delivery to the nodes of a communication medium. At last, non-repudiation mechanism represents the ability to give confirmable evidence of message delivery to the end nodes in order to make sure that the dispatcher and

receiver of a message cannot refuse and have sent or received the message.

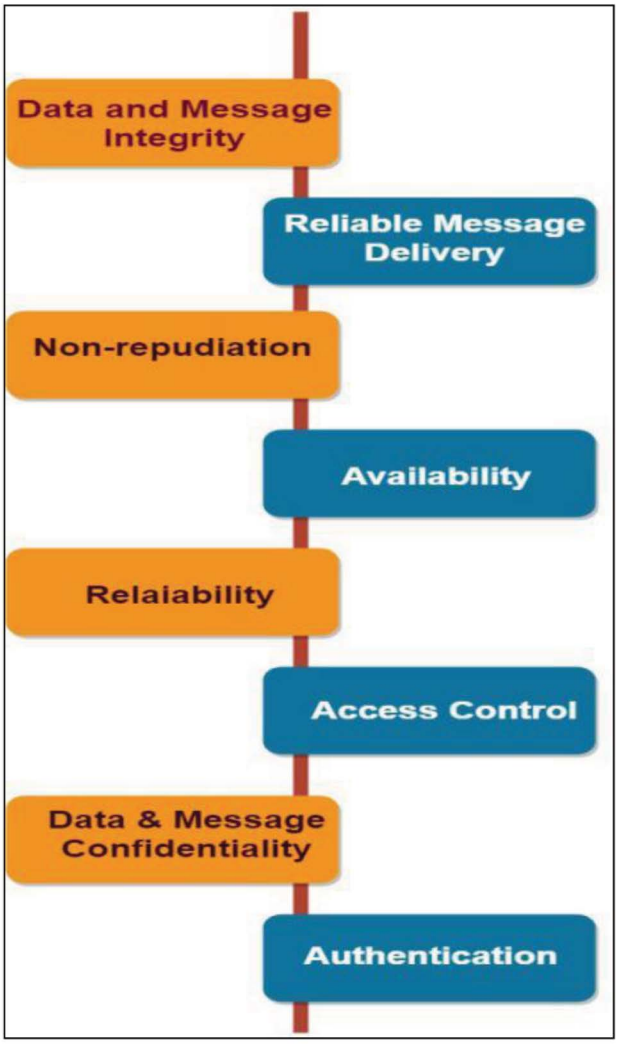

Figure 4. Basic requirements of security for financial systems.

4.2.2 Design Parameters of Wireless Security

In this sub-section, Authentication, Authorization, Secrecy Capacity, Intercept Probability, Complexity, Encryption and Latency are major factors as illustrated in Figure 5, which might kept in focus while designing the wireless security of Critical infrastructure systems such as financial system. At initial level, Authentication recognizes a client or user that is suitable to the explicit information and service. Then, transfer the rights to Authorization in identifying process of user to resources associated to information security and access controls. Secrecy Capacity is dynamic approach, it play utmost function to measure possible ideal secrecy rate and intercept probability. Simply, Intercept Probability is the possibility to seize or stop the function of service and technology. It performs requested function as intrusion, or target is reported as malicious at the execution level of system. Complexity, Encryption and Latency are inter-related to each other. The increase in user may increase complexity feature which is involved in a complex progression.

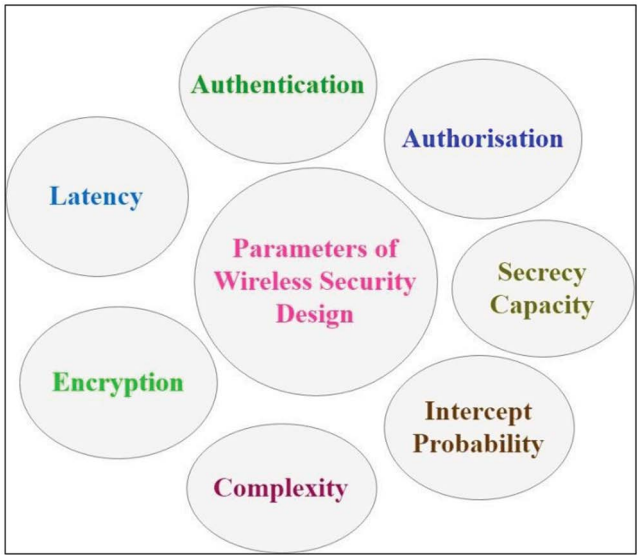

Figure 5. Design parameters of wireless security.

Though, the encryption technique performs the function to exchange and transform the plain text into cipher text for protection and security purpose. Higher the security, higher the encryption level requires. Thus, more complexity and encryption may require more time duration while sharing or communication. Moreover, Latency describes the delays prior to convey data or information which follows predefined instruction for procedure.

4.2.3 Algorithms and Techniques

This sub-section is most important part of proposed model because it depends upon techniques, which are focused to provide more secure and reliable framework. Thus, the professionals and experts rely on these security techniques which are as: Information Theoretic security, Security diversity methods, Artificial Noise aided security, Physical layer secret key generation and Security oriented beam forming shown in Figure 6.

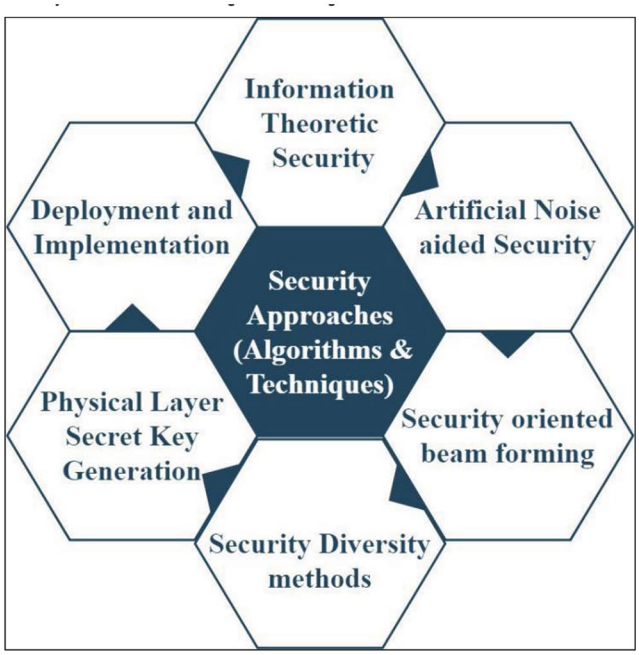

Figure 6. Security algorithms and techniques.

While discussing about Information Theoretic Security, following three basic wiretap channels would be identified. Such as: Memory less, Gaussian, and fading. Although, the third and latest channel named as "fading Wiretap Channel" is recommended for this proposed system. In this channel, a genuine transmitter and receiver both desires to link a secure and reliable communication of information theoretically in the existence of a spy. The wiretap channel was initially introduced for noiseless channels and demonstrated to protect the keys. Further, one-time-pad encryption is necessary and playing utmost role in secure communications via fading wiretap channel[21]. Artificial Noise aided security is also based on two approaches such as: Artificial noise design, power allocation. Generally, artificial noise design is the design of artificial noise, which is generated by a human source. The purpose of designing artificial noise is to depend on measured noise in a particular perspective. So, it is used to conduct a test of an issue by calculating the frequency of the artificial noise to determine how the subject cooperates with exterior motivation. Besides this, power allocation is a practice used to allocate the total existing power at the transmitter along the diverse antennas as well as maximize the performance metric. For example: the ergodic capacity. Both approaches have been recommended and proposed for financial system[22].

There are various security oriented beam forming such as Transmit beam forming, Receive beam forming and Collaborative beam forming. This study recommended collaborative beam forming for financial system. Collaborative beam forming is applicable in signal processing methods and sensor arrays for directional signal transceiver. Furthermore, collaborative beam forming can be applicable at both ends in order to accomplish spatial selectivity. The development contrasts with omni-directional transceiver, which is identified as the directivity of the array. Collaborative beam forming is also a power-efficient communication method that boosts the transmission range via bunch of sensor nodes. Though, it takes over several confronts from the scattered nature of WSNs[23,24].

Cooperative diversity is also recommended for financial system. Cooperative diversity is a supportive in manifold antenna practice to improve and maximize entire network channel capacity for specified bandwidths. The defined bandwidth develops user variety and then by deciphers the joint and direct signals of the relayed in the multi-hop wireless networks. A conventional single hop system employs direct communication where a receiver decodes the data which is based on the direct signal. Cooperative diversity decodes the information by grouping two signals together.

Therefore, it is noted that cooperative diversity is also antenna diversity, which is applicable in a wireless network that scattered antennas used to connect the nodes to each other. Though, user cooperation becomes a supplementary definition for cooperative diversity. The cooperative diversity is also a type of multi-user MIMO system[23]. Relay Channel is also used in key Extraction, which is also an important approach in the generation of secret key at Physical layer. In information theory, a Relay Channel based key extraction is a possibility form of the communication among transceivers via intermediary relay nodes. In this scheme, the relay forwards an amplified signal in the final time slot at receiving side[25]. Audio Frequency needs fewer delays as the relay node functions time-slot by time-slot. Thus, it consumes less power because decode or quantize operation is not achieved at the relay side.

5. Conclusion

Globally, cyber security of CI has become a primary and fragile theme in the last decade. So, Information sharing of Incident is an essential endeavor for potential

infrastructures. Though, a huge number of relatively various features require to be considered consecutively to execute and scamper efficient systems, which have been tackled in this paper. Moreover, the authors have proposed a framework to enhance the security level of financial systems. The proposed framework includes two major parts. First part is about enhanced Network Standards for the Security of System while second part illustrates architecture of the proposed framework. Network Standards supports the framework by defining security approaches and their parameters. In addition, the architecture comprised of three stages. Stage one comprises basic Security requirements, Stage two defines parameters of Wireless Security design and the last stage deploy security algorithms and techniques. Due to this proposed framework, this research is supportive for CI systems and helpful for the researchers and technologists while developing, designing such type of framework. This paper is recommended for the security of CI Financial System in which various emerging challenges have been identified and includes Identity Access controls , Monitoring, Risk investigation and administration, Service Level Understanding, Accounting, Heterogeneity, Virtualization, Compliance, Trust Administration, Cross-Hierarchical Security Administration, Policies, Security in the web program and proposed model comprised of expanded digitization and mechanization, expanded innovative capacities and simple accessibility of avionics information.

6. References

1. Singh M, Halgamuge MN, Ekici G, Jayasekara CS. A Review on Security and Privacy Challenges of Big Data. Cognitive Computing for Big Data Systems Over IoT; 2018. p. 175-200. https://doi.org/10.1007/978-3-319-70688-7_8.
2. Skopik F, Settanni G, Fiedler R. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing, Computers and Security. 2016; 60:154-76. https://doi.org/10.1016/j.cose.2016.04.003.
3. Wang X, Tehranipoor M, Plusquellic J. Detecting malicious inclusions in secure hardware: Challenges and solutions. IEEE International Workshop on Hardware-Oriented Security and Trust; 2008. p. 15-19.
4. Jang-Jaccard J, Nepal S. A survey of emerging threats in cyber security, Journal of Computer and System Sciences. 2014; 80(5):973-93. https://doi.org/10.1016/j.jcss.2014.02.005.
5. Awan JH, Memon S, Shah M, Awan FH. Security of eGovernment Services and Challenges in Pakistan. SAI Computing Conference (SAI); 2016. p. 1082-85. https://doi.org/10.1109/SAI.2016.7556112.
6. Awan J, Memon S. Threats of Cyber Security and Challenges for Pakistan. 11th International Conference on Cyber Warfare and Security: ICCWS - 2016, Boston USA. 2016. p. 425.
7. Awan JH, Memon S, Pathan SM, Usman M, Khan RA, Abbasi S. A user friendly security framework for the protection of confidential information, International Journal of Computer Science and Network Security. 2017; 17(4):215-23. https://doi.org/10.1016/S1353-4858(17)30090-9.
8. Awan JH, Memon S, Khan RA, Noonari AQ, Hussain Z, Usman M. Security strategies to overcome cyber measures, factors and barriers, Engineering Science and Technology, an International Journal. 2017; 1(1):51-58.
9. Awan JH, Memon S, Memon S, Pathan KTAJ, Arijo NH. Cyber Threats/Attacks and a Defensive Model to Mitigate Cyber Activities, Mehran University Research Journal of Engineering and Technology. 2018; 37(2):359-66. https://doi.org/10.22581/muet1982.1802.12.
10. Memon SA, Awan JH. Transformation towards Cyber Democracy: A study on Contemporary Policies, Practices and Adoption Challenges for Pakistan. Handbook of Cyber-Development, Cyber-Democracy and Cyber-Defense; 2017. p. 1-20. https://doi.org/10.1007/978-3-319-06091-0_50-1. PMid: 28116554, PMCid: PMC5256624.
11. Amoroso E. Cyber Security [Internet]. 2006. Available from: http://books.google.com/books?id=kwTrAAAACAA
12. Devries PD. An Analysis of Cryptocurrency, Bitcoin, and the Future, International Journal of Management and Commerce Innovation. 2016; 1(2):1-9.
13. Alarifi A, Alsaleh M, Alomar N. A model for evaluating the security and usability of e-banking platforms, Computing. 2017; 99(5):519-35. https://doi.org/10.1007/s00607-017-0546-9.
14. Liu L, De Vel O, Han QL, Zhang J, Xiang Y. Detecting and Preventing Cyber Insider Threats: A Survey. IEEE Communications Surveys and Tutorials; 2018. p. 1-21. https://doi.org/10.1109/COMST.2018.2800740.
15. Abughazalah S, Markantonakis K, Mayes K. Secure mobile payment on NFC-enabled mobile phones formally analysed using Casper FDR. IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications; 2015. p. 422-31. https://doi.org/10.1109/TrustCom.2014.55.
16. Nespoli P, Papamartzivanos D, Marmol FG, Kambourakis G. Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks, IEEE

Communications Surveys and Tutorials. 2017; 20(2):1361-96. https://doi.org/10.1109/COMST.2017.2781126.
17. Mahmadi FN, Zaaba ZF, Osman A. Computer Security Issues in Online Banking: An Assessment from the Context of Usable Security, IOP Conference Series: Materials Science and Engineering. 2016; 160(1):1-12. https://doi.org/10.1088/1757-899X/160/1/012107.
18. Li X, Eckert M, Martinez J, Rubio G. Context Aware Middleware Architectures: Survey and Challenges, Sensors. 2015; 15:20570-607. https://doi.org/10.3390/s150820570. PMid: 26307988, PMCid: PMC4570438.
19. Tahir M, Qureshi R, Ahmed S. A Survey of Energy Conservation Mechanisms for Dynamic Cluster Based Wireless Sensor Networks, Mehran University Research Journal of Engineering and Technology. 2018; 37(2):279-314. https://doi.org/10.22581/muet1982.1802.05.
20. Automating Cyber Offensive Operations for Cyber Challenges. Date accessed: 03/2016. https://pdfs.semanticscholar.org/575f/5a9de2eeef22b2fdb950abf9eb16b1f48e9e.pdf.
21. Zhang X, Zhou X, McKay MR. On the Design of Artificial-Noise-Aided Secure Multi-Antenna Transmission in Slow Fading Channels; 2012. p. 1-12.
22. Khoshnevisan M, Laneman JN. Power Allocation in Wireless Systems Subject to Long-Term and Short-Term Power Constraints. IEEE International Conference on Communications (ICC); 2011. p. 1-5. https://doi.org/10.1109/icc.2011.5963208.
23. Ahmed MF. Collaborative beam forming for wireless sensor networks with Gaussian distributed sensor nodes, IEEE Transactions on Wireless Communications. 2009; 8(2):638-43. https://doi.org/10.1109/TWC.2009.071339.
24. Awan JH, Memon SA, Memon NA, Shah R, Bhutto Z, Khan RA. Conceptual Model for WWBAN (Wearable Wireless Body Area Network), International Journal of Advanced Computer Science and Applications. 2017; 8(1):377-81. https://doi.org/10.14569/IJACSA.2017.080147.
25. Liao WC, Chang TH, Ma WK, Chi CY. QoS-based transmit beam forming in the presence of eavesdroppers: An optimized artificial-noise-aided approach, IEEE Transactions on Signal Processing. 2011; 59(3):1202-16