

Evaluation of ICT Security Implementation in Banks: Bangladesh Perspective

Md. Saddam Hossain Remus^{1,2}, Sanzida Akter^{3,4}, Khaleda Ferdous^{5,6}

¹B.Sc. in EEE (IUBAT - International University of Business Agriculture and Technology)

²Masters in Information Technology (IIT, Jahangirnagar University)

³B.SC. in EEE , United International University

⁴MBA , University of Asia Pacific

⁵Bachelor's degree in Computer Science & Engineering, Institute of Science & Technology of National University Bangladesh,

⁶ Master's degree in Computer Science, Jahangirnagar University, Bangladesh.
amambagdadee@gmail.com

doi: <https://doi.org/10.37745/ejcsit.2013/vol11n62241>

Published December 18 2023

Citation: Remus M.H.S., Akter A., Ferdous K. (2023) Evaluation of ICT Security Implementation in Banks: Bangladesh Perspective, *European Journal of Computer Science and Information Technology*, 11 (6), 22-41

ABSTRACT: *Nowadays, banks are the foundation of a strong economy in any country, whereas information and communication technology (ICT) has become the heart of any bank. As a result, one of the major challenges has become ensuring the security of the banks. Whenever ICT security comes up, the foremost thing that needs to be considered is " PAM, PCI DSS, SIEM, and ICT risk management," which measures are improving immensely day by day. Under the ICT security guidelines of Bangladesh Bank, all banks are implementing many security measures to ensure ICT security standards. This paper mainly emphasis on the implementation of ICT security measures such as PAM, PCI DSS, SIEM, and ICT risk management through surveys from different banks. It also focuses on the challenges and future prospects of ICT security measures.*

KEYWORDS: ICT security measures, PAM, PCI DSS, SIEM, ICT risk management, Survey, Python

INTRODUCTION

In the last few years, the banking sector has reformed its methods of providing different types of services to its customers and handling data. This historic trans-formation has been brought about by information and communication technology (ICT). Furthermore, the information security measures (PAM, PCI-DSS, SIEM and ICT Risk Management) for financial institutions have grown in importance, and it is critical that the risks or threats are correctly addressed and controlled. Securing assets are the main concern to any organization's long-term viability. And banks should be responsible for preventing unauthorized access to the systems, modification of data and disclosure of information [1]. Therefore, Bangladesh Bank's ICT Security guidelines help to implement and practice ICT security measures to make sure confidentiality, integrity and availability of information. With this background, this research project tries to explore the situation of information security measures, challenges in safeguarding them, and proposes some future initiatives.

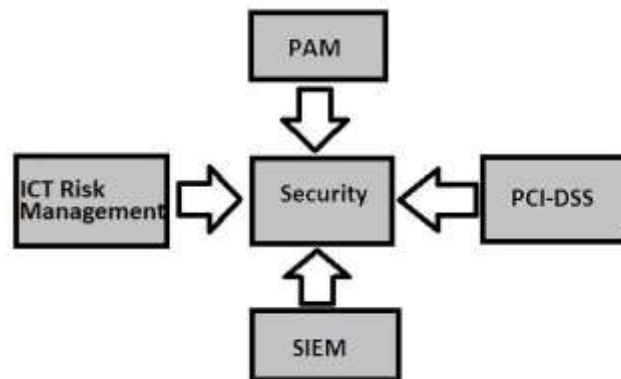


Figure 1. Research Interest in Field of ICT security measures

The most difficult task is to prioritize new technologies over traditional ones. A data survey from the banks is required to understand the present status of banks' ICT security measures such as PAM, PCI-DSS, SIEM, and ICT risk management. According to the Bangladesh Bank's ICT guidelines, a data survey is required from different banks. The outcome of data analysis represents the existing security infrastructure, security gaps and the recommendation for the future. For further investigation, the primary concern is data collection and analysis from different banks of ICT security measures. Analyzing research interests and current activity in the area of ICT security in the banking sector of Bangladesh, which is considered a national security issue, drives the researcher towards the field. As information and communication technology (ICT) become more important, security has become a major challenge for banks. Interest in this field is proportionally increasing with the significance of this domain. From figure 1.1 shows the research interest in four major ICT security measures comes from many of them being guided by the Bangladesh Bank for protection of the financial sector from cybercrime and risk. This drives us to analysis of the present and future achievement of ICT security measures in banks. The research study is based on identifying the significance of ICT security in banks to protect them from cybercrimes and losses. The following are some of the specific goals of this thesis that should be mentioned:

- To analyze adoption of ICT security measures in banks.
- To identify shortcomings in the implementation of ICT security measures.
- To make necessary recommendations to overcome the problems.

LITERATURE REVIEW

2.1.Related Work

This section examines relevant literature as well as previous research findings on ICT security in banks. The studies conducted in the context of developed and developing countries are presented here to highlight existing knowledge. Reference [1-3] discussed from password management to least privilege management and secure remote access, the Privilege Management paradigm

involves safeguarding and controlling privileges throughout the entire landscape. The privileged security challenge can only be fully handled by enabling this holistic approach and the three key PAM disciplines (Privileged Password Management, Endpoint Privilege Management, and Secure Remote Access). Reference [4,5] provided an overview of the Payment Card Industry's (PCI) ostensibly coordinated attempts to develop standardized data security standards, known as PCI DSS. The PCI DSS may indeed provide consumers with enhanced security. The training and credentialing services conducted by PCI SSC have the ability to increase uniformity in the application of data security requirements. A QSA's certification will be recognized by all of the founding payment card brands. Reference [6,7] introduced enterprise SOCs are organized in a hierarchical manner around SIEM systems. The SIEM system sends out notifications and triages events, determining whether they're real threats or false alarms. If a rule generates a high number of false positives, level 1 SAs escalate it to a SOC engineer or a higher-level SA for further tuning to decrease false positives. When level 1 SAs are unable to determine whether an alert is an attack or a false positive, the alert is escalated for further investigation. Reference [8] discovered the data to be gathered, the formulation of the data form, and the processes employed by the observer or interviewer during the data gathering process are the three components of data collection. Another crucial aspect is the ability to obtain information. The responders are willing and able to respond if it is a questioning procedure. An observer can be expected to accurately observe the action in an observation study. In Reference [9], the survey procedure is discussed. The questionnaire inquired as to whether or not various organizational measures had been applied. Some of these initiatives were complemented by more in-depth questions about their application. In addition, respondents were asked to subjectively rate the efficiency of certain measures, regardless of whether they had been implemented or not, as well as explain what they believed the effectiveness of information security measures to be. The poll also included questions about the organization's perceived information security performance. Reference [10] used the category selection method of banks under the BB ICT guidelines. Categories are measured depending on the score obtained by the banks. The category indicates the compliance level of the banks. This paper [12] explored the nature of qualitative data and its tumultuous connection with computer-assisted analysis. However, analyzing such data is difficult and time-consuming, and there is a lack of precise guidance on how to go about it. This work [14] proposed credentials to provide access control. In computer systems, user access levels are determined or assigned to credentials by a person with administrative rights. Privileged access management would include any user with access to a system above and beyond that of a regular user. Reference [15] presented Banks' performance is judged by measures of profitability and asset quality, while information security is measured by the extent to which PCI-DSS standards are applied to them. The Payment Card Industry Data Security Standards (PCI-DSS) is a comprehensive standard designed to assist businesses in safeguarding consumer account information. This research [16] introduced SIEM (Security Information and Event Management) systems have become popular as a strong tool for preventing, detecting, and responding to cyber-attacks. SIEM systems have evolved into comprehensive systems that provide broad insight to detect high-risk regions and proactively focus on mitigation methods to reduce incident response costs and time. This paper [17] presented an examination of the challenge of deciding how much to invest in information security. The study resulted in a recommendation that could eventually become a standardized method. This paper [18] explored how Privileged Access Management (PAM) is commonly used in today's networks to manage administrative access to Linux servers (PAM). Typically, security management processes use adaptation to continuously improve products, services, or processes within the network infrastructure. Reference [19] discussed PCI DSS is a data security standard that applies to any firm

that processes cardholder data from major credit card companies including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. PCI DSS's major priority, as outlined in their data security compliance processes, is data security. PCI DSS compliance is required of every entity that keeps, processes, or transmits cardholder data. The PCI DSS outlines optimal security practices that can be implemented as common sense measures to safeguard an organization's information assets. In Reference [20], In a real-world industry system, SIEM is used. Analysis provides the way for data discovery methodologies as a viable route to augment the current SIEM practice while dealing with a practical industry challenge. Reference [21] demonstrated that the use of ICT improves the bank's image while also allowing for a larger, faster, and more efficient market. It has also made work easier and more exciting, boosted banks' competitiveness, strengthened customer connections, and aided in the resolution of basic operational and planning issues.

2.2 Privileged Access Management (PAM)

Protection from the risks of the theft of credentials and exploitation of the privilege, banks use privileged access management (PAM). PAM is a comprehensive cyber security approach that includes users, procedures, and technology for controlling, monitoring, securing, and auditing all types of privileged identities and actions in banks IT systems [22]. Protecting, managing, and monitoring privileged access presents a number of issues for organizations, including: Account credentials management: To cycle and update privileged access credentials, banks depend on manual activities, error-prone administrative systems. This is a time-consuming and costly method. Monitoring and controlling privileged sessions: Banks are not capable of centrally monitoring and controlling privileged sessions, leaving them vulnerable to cyber security violations.

Threat detection and analysis: Banks have the shortage of comprehensive security tools and that making the difficulties of suspicious activity detection and resolve the incidents. Access Privileges: Sometimes organizations struggle to identify the privileged users to cloud platforms (IaaS and PaaS and SaaS) applications and other resources, resulting in compliance and operational risks. Defending the domain controllers: By exploiting weaknesses, attackers can take access to vital ICT resources, confidential data and disable the Kerberos authentication system for certain period.

2.2.1 PAM architecture

Privileges should be secured across all users, sessions, and assets in a PAM architecture and that is considered successful. Traditionally, all services provided by the automated credential management solution, is the main key of a PAM solution that enterprises aim to implement. There are two more important aspects of PAM solution whereas first one is the least privilege management and second one is the remote access management. For the entire privilege premises, these three solutions should be connected and work together [23]. Here, shown an example of PAM architecture.

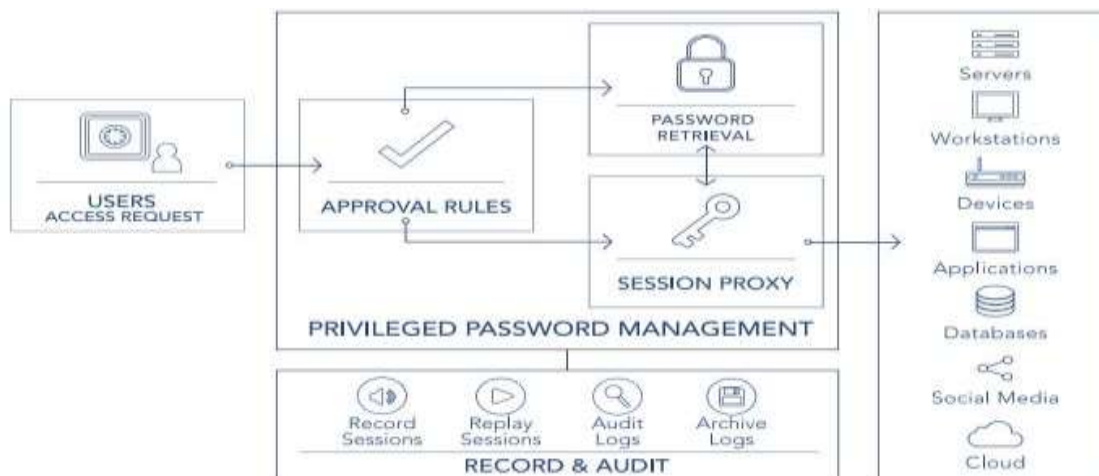


Figure 2. Privileged Access Management

2.3 Payment Card Industry Data Security Standard (PCI DSS)

In order to ensure security, PCI DSS is the standard for payment systems of any organization that uses different branded cards, and they generate a lot of payment related data. The PCI SSC administers the PCI Standard, which is mandated by the card brands. To combat credit card fraud, the standard was established to tighten safeguards surrounding cardholder data [24].

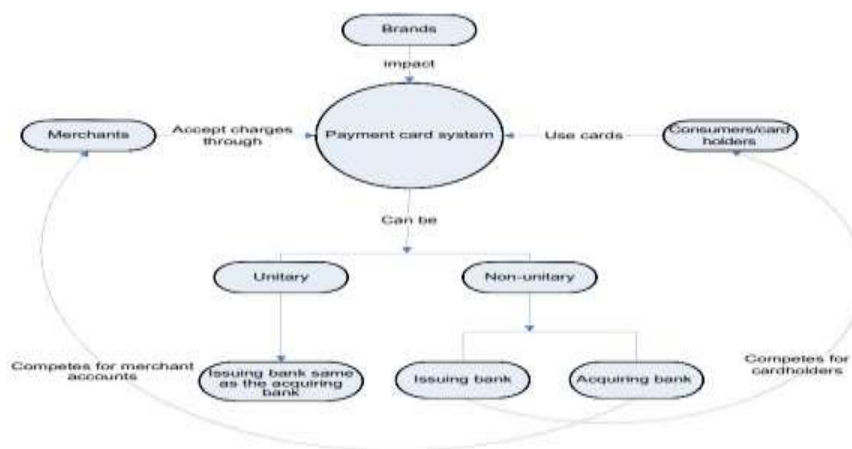


Figure 3. Payment Card Industry Features

From figure 2.2 In addition, the use of payment cards is reliant on the interactions of two key groups: customers and merchants. Comprehending these interrelationships, as well as the framework that is a good starting point for understanding security methods. The PCI DSS is required for banks that offer payment cards for brands such as Visa, Mastercard, Discover and American Express. Any institute or entity that handles or deals with card data from one of the five major card brands, for that matter, must adhere to PCI DSS criteria. [25].

2.4 Security Information and Event Management (SIEM)

In the domain of ICT security, security information and event management (SIEM) plays an important role. It helps to analyze security alarms generated by applications and network devices. The results show in real time. It is available as software, equipment and managed services and it generates security log data and also generate compliance reports [26].

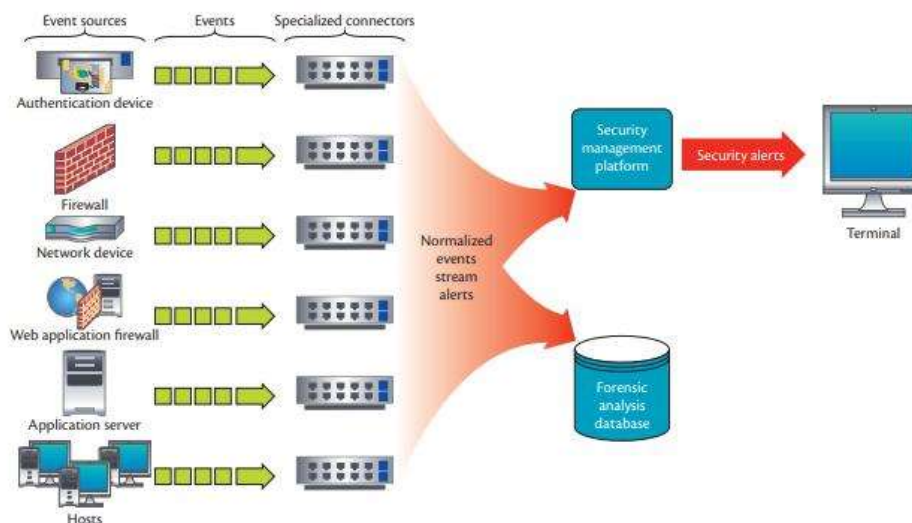


Figure 4. SIEM architecture

In addition, SIEM systems are the main a component for SOCs to collect, stan-dardize and analyse security events from different sources. But it also adapt to address further scalability concerns. Various security devices and sensors send data to the SIEM system. Connectors take the events then analyse and form in different standard ways [27].

3. System Model

3.1 Preparation of questionnaires

Generally, Preparation of questionnaires depend on the system model of the re-search goal. The selection starts with reviewing the parameters and following the guidelines. Preparation of questionnaires has the three phases of the data collection process that depend on the basic data collection technique [28]. Preparation of questionnaires refers to identifying communication variables as per Bangladesh Bank guidelines that influence performance.

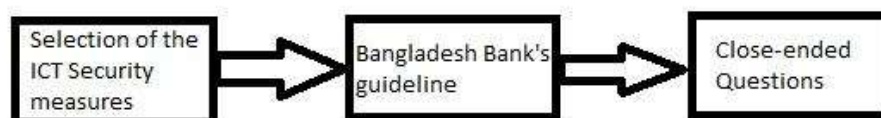


Figure 5. Figure 3.1 Preparation of questionnaires.png

According to figure 5, the primary task is to select ICT security measures such as PAM, PCI-DSS, SIEM, and ICT risk management. Then, to identify communication variables, follow the Bangladesh Bank's ICT guidelines. Finally, the questionnaire is prepared using closed-ended questions.

3.2 Data Collection

The research questionnaires were answered by examining the responses of 10 different banks' information security officers and managers. The questionnaire inquired as to whether or not various organizational measures had been applied. Some of these initiatives were complemented by more in-depth questions about their application. Data has been collected after ensuring the confidentiality of a bank information also. The current study investigate the relationships between implementation of measures and their effectiveness. It also depends on the sample size [9]. Furthermore, the methods and goals of each field may differ, the overall process of data collection remains largely the same. Before beginning to collect data, the following must be considered:

- The aim of the research study
- The type of data that will be collected
- The procedures and methods that will be used to collect, store, and process data include

3.3 Category Selection

In this study, the findings are organized into 5 categories following the Bangladesh Bank's ICT guidelines [10]. The categories can be divided into groups, each of which corresponds to a different set of variables. The categories should be extensive, since they should encompass all of the variables and elements reserved in our design for resolution using the content analysis technique. The ICT security of a bank may be judged from different points of view, but emphasis has to be given to the feasibility of the aspects being considered for implementation and its practice. These are based on scores, which are given below:

- If the score is 90% or above, it will be marked "Excellent".
- If the score is 80% or above but below 90%, it will be marked as "Very Good".
- If the score is 70% or above but below 80%, it will be marked as "Good".
- If the score is 60% or above but below 70%, it will be marked as "Satisfactory".
- If the score is below 60%, it will be treated as "Marginal".

The above mentioned categories influence the final results. The performance and result analysis also initiate based on the category selection to get the findings of this evaluation.

3.4 Methodology workflow

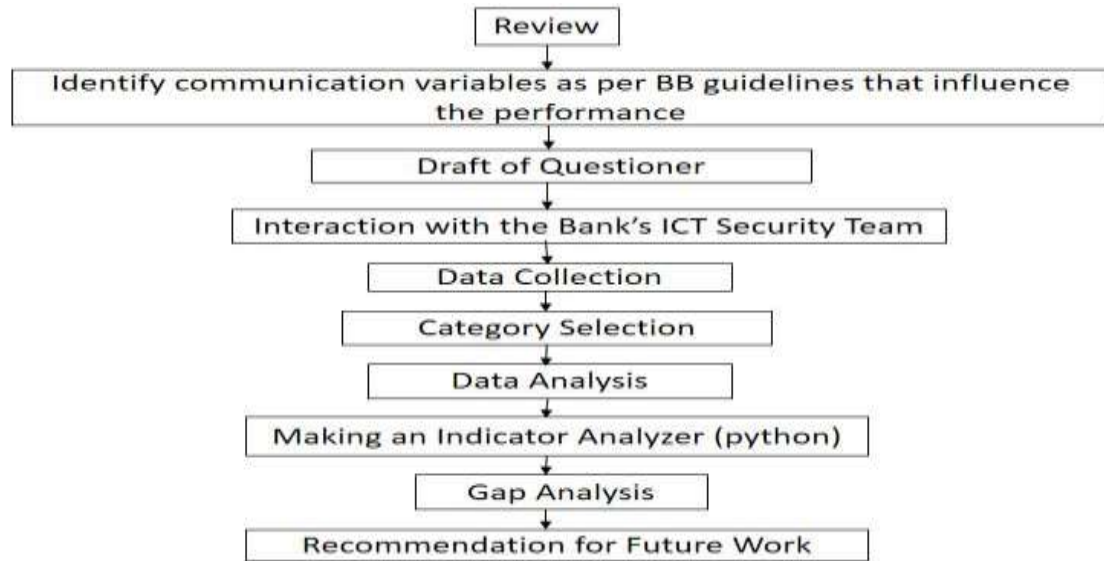


Figure 6. Methodology workflow

4. Data Analysis

4.1 Data Analysis

Data analysis is defined as the process of manipulating some sort of data or information for a certain result. Applying the statistical and the logical process to understand the data is known as data analysis. According to Shamoo and Resnik, there are different analytic methods applied to understand the data. [11]. There are three steps for the data analysis process. The first is organization and The second is summarization and classification and the third is analysis of the data.

4.2 Data analysis methods

4.2.1 Qualitative Analysis

Quantitative uses 'why' 'what' and 'how' to find the answers. To find the little is known subject a qualitative approach may be employed [12]. Rather than testing theory, It's more likely that the objective will be inductive. Quantitative analysis defines the numerical results obtained by manipulating data [13]The three primary methodologies for measuring data are regression analysis, lin-ear programming, and data measuring. Here, the qualitative analysis method was chosen for this research to get a precise out

4.3 Data and Questionnaire

Here, the questionnaire of the survey has been designed using 90 questions which is related to the study. A three point “Yes”, “No” and “In progress” was used as the scale of measurement for each question (close-ended) in the questionnaire. Analysis of the study is done with the help of the relevant techniques. The data has been analyzed by using MS-Excel 2013 and python software. The analysis represents the current status and security gaps of the ICT security measures.

4.4 Score for ICT Security Measures of different Banks

ICT security is the prime concern of the banks. PAM, PCI-DSS, SIEM, and ICT Risk Management are the major keys among all the ICT security measures in banks. These four measures help to grow business efficiently. However, the survey shows the data collected from the different private banks in Bangladesh, including 1st, 2nd, 3rd, and 4th generation banks. Due to security and confidentiality, the bank names correspond to Bank 1, Bank 2, Bank 3, Bank 4, Bank 5, Bank 6, Bank 7, Bank 8, Bank 9, and Bank 10 respectively. The data table shows the mean score of the close-ended questions. The percentage of satisfaction values for each question/parameter was compared with a reference score of “100”, which was considered the maximum that any organization should like to achieve for excellence. The following table shows the status of the scores for ICT security measures for different banks. From Table 1, the bank names correspond to B 1, B 2, B 3, B 4, B 5, B 6, B 7, B 8, B 9, and B 10 respectively, with the Name of Security Measures as NSM.

Table 1: Mean Score for ICT Security Measures of Banks

NSM	B 1	B 2	B 3	B 4	B 5	B 6	B 7	B 8	B 9	B 10
PAM	52.27	86.36	86.36	86.36	52.27	52.27	86.36	52.27	86.36	27.27
PCI-DSS	60.53	84.21	84.21	60.53	60.53	60.53	60.53	60.53	84.21	2.63
SIEM	26.67	100	100	100	26.67	26.67	100	26.67	100	26.67
ICT RM	67.65	97.06	91.18	97.06	67.65	67.65	97.06	67.65	97.06	67.65

4.5 Stages of Implementation Analysis

4.5.1 Privileged Access Management (PAM)

In banks, security breaches are becoming more regular. Therefore, the use of privilege access management in banks for security objectives will be examined in detail [14]. Identity-management systems, products, programs, and platforms manage identifying and auxiliary data for individuals, computer-related devices, and software applications, among other entities. For data collection, below mention parameters are the major concern. From figure 7, it is clear that banks are trying to follow the guidelines imposed by the Bangladesh Bank. The percentage of satisfaction values for each question/parameter was compared with a reference score of “100”, which was considered the maximum that any organization should like to achieve for excellence.

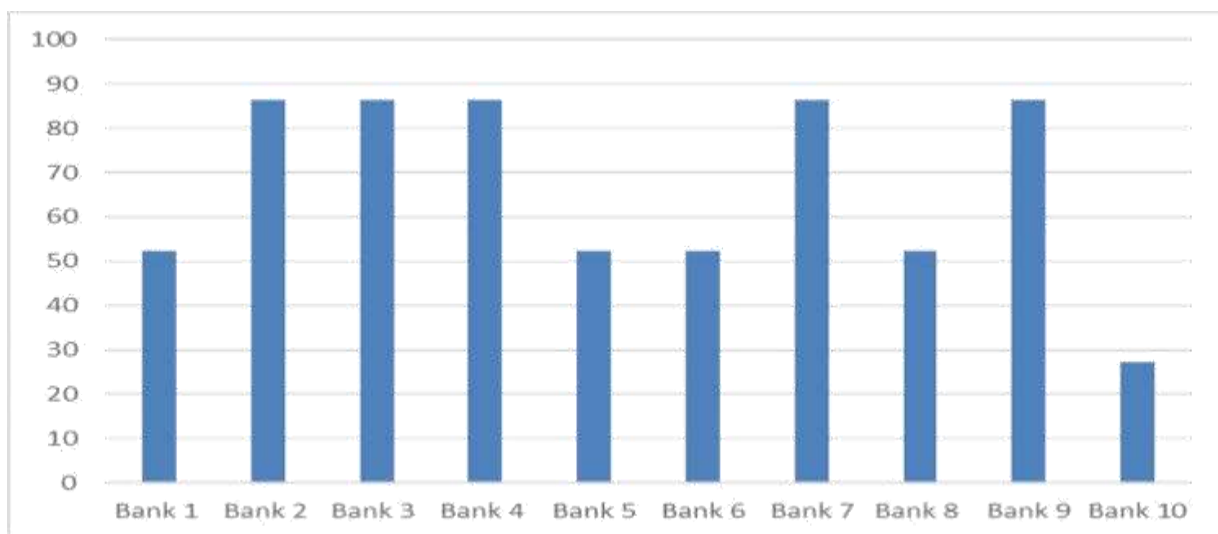


Figure 7. PAM score status of different banks

4.5.2b Payment Card Industry Data Security Standard (PCI DSS)

It is the standards which are applied to the banks to ensure customer data security

PCI compliance is categorized into four levels based on the annual quantity of credit or debit card transactions done by a company Level (L1, L2, L3 and L4). The level determines what an organization must do to remain compliant. From figure 8, it is clear that banks are trying to follow the guidelines im-posed by the Bangladesh Bank. The percentage of satisfaction values for each ques-tion/parameter was compared with a reference score of "100", which was considered the maximum that any organization should like to achieve for excellence.

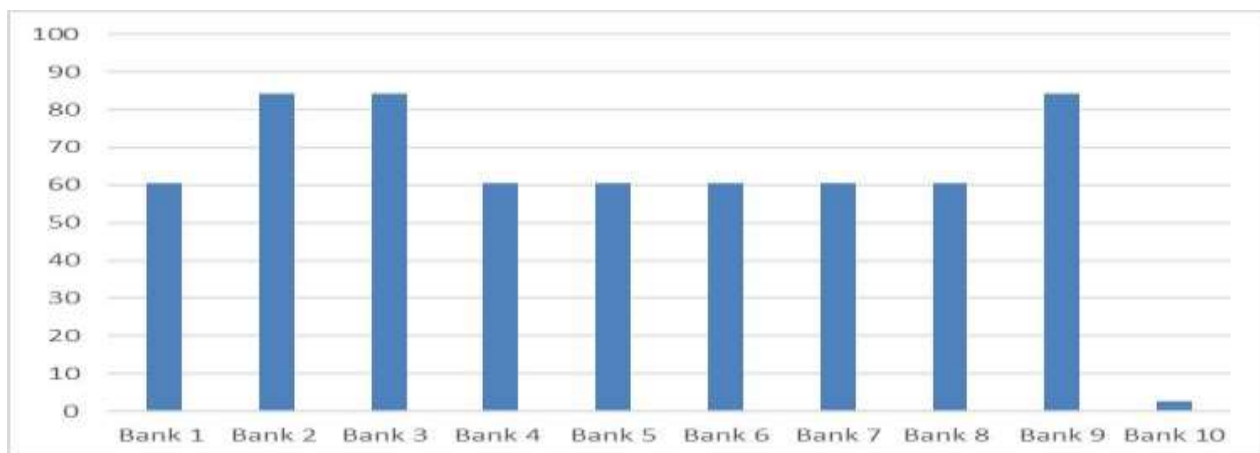


Figure 8. PCI DSS score status of different bank

4.5.3 Security Information and Event Monitoring (SIEM)

SIEM system is responsible for gathering, aggregating, storing, and correlating events created by a managed infrastructure. It collects data from many sources such as anti-virus, intrusion/prevention detection systems, firewalls and so on. Then correlate them and generate threat alerts with security reports [16]. This research focus is based on some parameters that are guided by the central bank.

From figure 9, it is clear that banks are trying to follow the guidelines imposed by the Bangladesh Bank. The percentage of satisfaction values for each question/parameter was compared with a reference score of "100", which was considered the maximum that any organization should like to achieve for excellence.

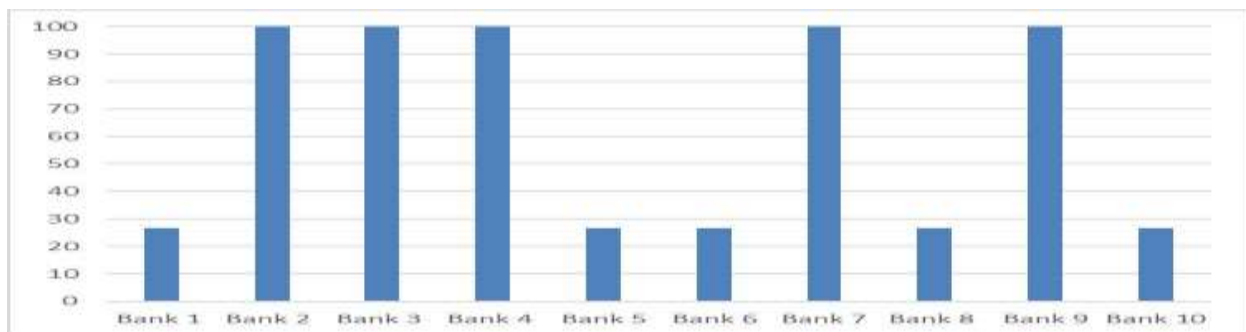


Figure 9. SIEM score status of different banks

4.5.4 ICT Risk Management

ICT risk management is to identify, measure, and respond to risks so that decision-making can be informed. Risk analysis requires knowledge of the organization's information assets to find out the assets' vulnerability and to mitigate the risk which policy has been deployed[17]. It consists of Risk governance, Risk Management and Risk response under BB ICT security guidelines. From figure 10, it is clear that banks are trying to follow the guidelines imposed by the Bangladesh Bank. The percentage of satisfaction values for each question/parameter was compared with a reference score of "100", which was considered the maximum that any organization should like to achieve for excellence.

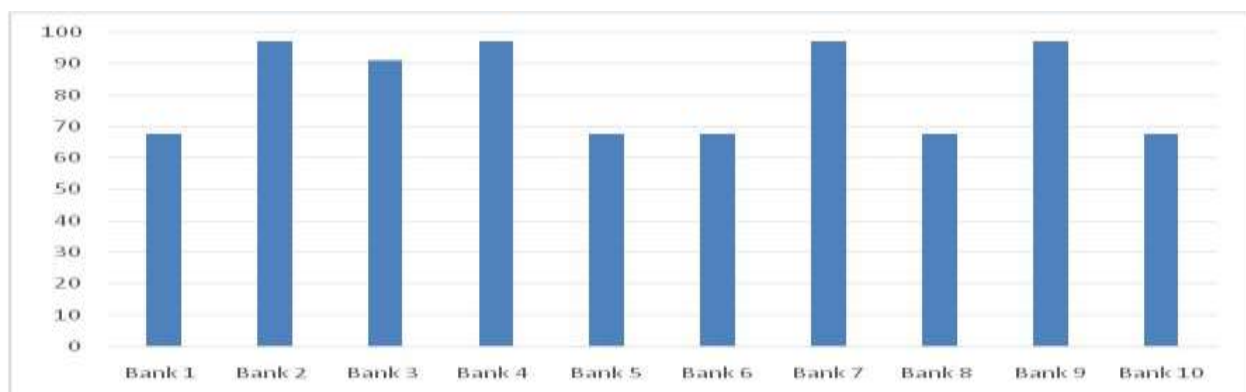


Figure 10. ICT Risk Management score status of different banks

4.6 Percentage analysis of security implementation

From figure 11, it is seen that 24% of PAM, 23% of PCI-DSS, 23% of SIEM, and 30% of ICT risk management have been implemented by the banks. The mean scores of PAM, PCI-DSS, SIEM, and ICT risk management are 66.82, 61.84, 63.34, and 81.77, respectively. Though it has the effectiveness but still it is required to set up these core security measures as early as possible to take the full benefits of today's tech-based banking and competitive and advantages.

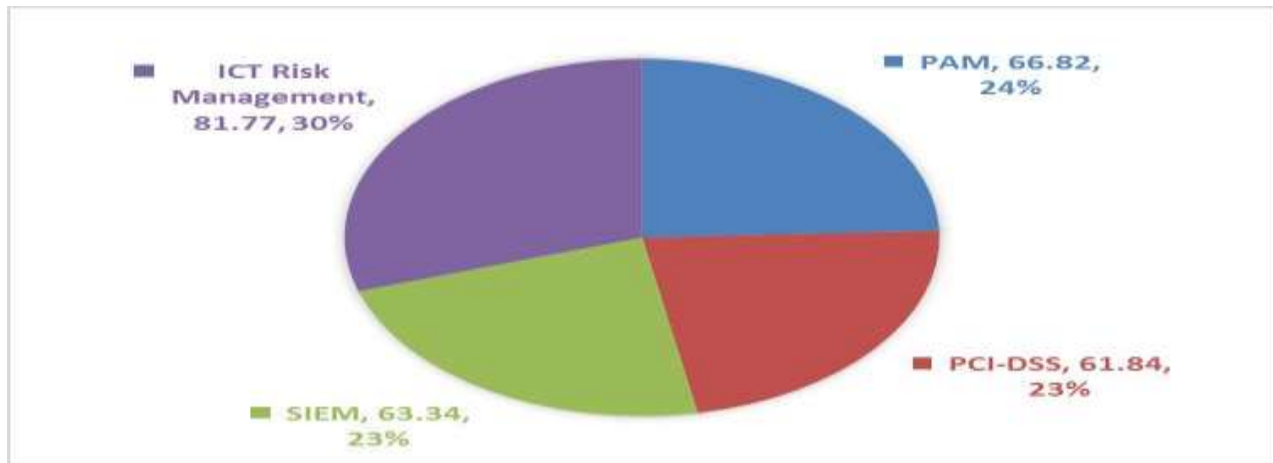


Figure 11. Percentage analysis of security implementation

5. Performance Analysis

5.1 Research findings from different banks

Bangladesh Bank is playing a vigorous role in the ICT security of the banking sector. As per Figure 12, the respondents indicate that Bangladesh Bank's ICT security guidelines help banks become more secure. And all the banks are struggling to implement and practice ICT security measures (PAM, PCI DSS, SIEM, and ICT Risk Management) to meet the security goal. According to the views of IT security professionals from different banks, they are trying to find out the factors that create barriers to constructing an effective information security program in different banks.

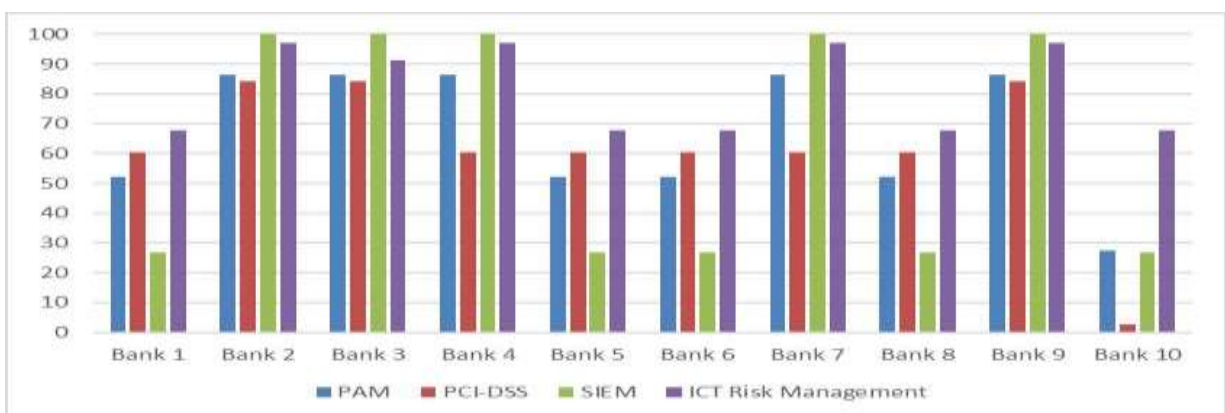


Figure 12. Research findings from different banks

As a result, expectations from BB have been increasing day by day, and banks have been demanding some important initiatives be taken by BB in the last few years.

5.2 Result Analysis by Python

Python is a perfect tool for evaluating performance. Therefore, this study uses "Python" as a tool for ICT security measures analysis. Here, Google Colab has been used for the writing and the execution of codes in Python version 3.7.12.

5.2.1 Flow chart

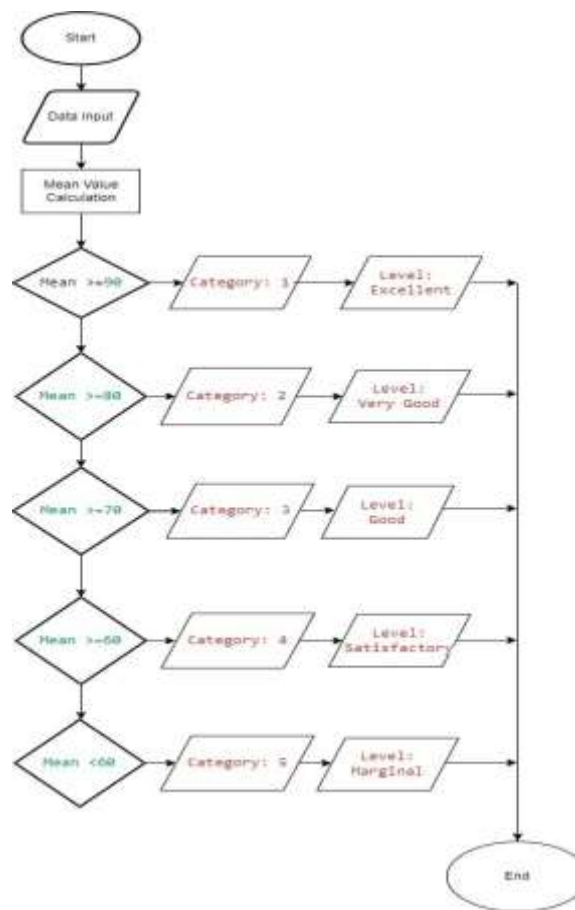


Figure 13 Flow Chart of coding

5.2.2 FINAL RESULTS

- PAM: From figure 14, the PAM data is provided as input from Table 4.1 by the 10 different banks, where the output comes as a mean value. After getting the mean value, the next step is the category selection using the score range from the score range table. Then the result

comes with a category and marked level. In this case, the category is 4 and the level is marked as Satisfactory.

```

Input Section:
Bank 1, Bank 2, Bank 3, Bank 4, Bank 5, Bank 6, Bank 7, Bank 8, Bank 9, Bank 10
[ ]

Output Section:
Bank 1, Bank 2, Bank 3, Bank 4, Bank 5, Bank 6, Bank 7, Bank 8, Bank 9, Bank 10
Score: (52.27, 86.36, 86.36, 86.36, 52.27, 52.27, 86.36, 52.27, 86.36, 27.27)
PAM : 66.815
Category: 4
Level: Satisfactory

```

Figure 14: PAM result using Python

- PCI DSS: Figure 15, shows the PCI DSS data is provided as input from Table 4.1 by the 10 different banks, where the output comes as a mean value. After getting the mean value, the next step is the category selection using the score range from the score range table. Then the result comes with a category and marked level. In this case, the category is 4 and the level is marked as Satisfactory.

```

Input Section:
Bank 1, Bank 2, Bank 3, Bank 4, Bank 5, Bank 6, Bank 7, Bank 8, Bank 9, Bank 10
[ ]

Output Section:
Bank 1, Bank 2, Bank 3, Bank 4, Bank 5, Bank 6, Bank 7, Bank 8, Bank 9, Bank 10
Score: (60.53, 84.21, 84.21, 60.53, 60.53, 60.53, 60.53, 60.53, 84.21, 2.63)
PCI DSS: 61.843999999999994
Category: 4
Level: Satisfactory

```

Figure 15 PCI DSS result using Python

- SIEM: Figure 16, visualizes the SIEM data is provided as input from Table 4.1 by the 10 different banks, where the output comes as a mean value. After getting the mean value, the next step is the category selection using the score range from the score range table. Then the result comes with a category and marked level. In this case, the category is 4 and the level is marked as Satisfactory

Input Section: Publication of the European Centre for Research Training and Development -UK

Bank 1, Bank 2, Bank 3, Bank 4, Bank 5, Bank 6, Bank 7, Bank 8, Bank 9, Bank 10

Output Section:

Bank 1, Bank 2, Bank 3, Bank 4, Bank 5, Bank 6, Bank 7, Bank 8, Bank 9, Bank 10:
 Score: (26.67, 100, 100, 100, 26.67, 26.67, 100, 26.67, 100, 26.67)
 SIEM: 63.335
 Category: 4
 Level: Satisfactory

Figure 16. SIEM result using Python

- ICT Risk Management: From figure 17, the ICT Risk Management data is provided as input from Table 4.1 by the 10 different banks, where the output comes as a mean value. After getting the mean value, the next step is the category selection using the score range from the score range table. Then the result comes with a category and marked level. In this case, the category is 2 and the level is marked as Very Good.

Input Section:

Bank 1, Bank 2, Bank 3, Bank 4, Bank 5, Bank 6, Bank 7, Bank 8, Bank 9, Bank 10

Output Section:

Bank 1, Bank 2, Bank 3, Bank 4, Bank 5, Bank 6, Bank 7, Bank 8, Bank 9, Bank 10:
 Score: (67.65, 97.06, 91.18, 97.06, 67.65, 67.65, 97.06, 67.65, 97.06, 67.65)
 ICT Risk Management: 81.767
 Category: 2
 Level: Very Good

Figure 17. ICT risk management result using Python

5.3 Security Gap Analysis under BB ICT Security Guide- lines

Following figure shows the gap between the current situation and highest expectation(100) considering ICT security guidelines of BB. This will help the management to reduce the gap between the real scenario and expectation.

- PAM: It is critical not only to monitor these privileged accounts, but also to control segregation of duties and detect keys and accounts that may bypass PAM [18]. Unrestricted access can pose a business risk of any organization. Here, the banks achieved 66.82 marks, which is a satisfactory standard. It is clear that still banks are far behind in meeting the excellence in this regard.
- PCI DSS: PCI DSS implementation is considered as successful when the information security of an organization is ensured securely, with cardholder data security being the primary issue [19]. In the case of this standard, banks scored 61.84, which is a satisfactory standard. It is clear that banks are still very weak in this particular field.
- SIEM: SIEM is the process or system of handling data from different sources or devices. Here, although addressing a practical issue, lays the path for creative techniques to

supplement current SIEM practice [20]. But the condition of banks in meeting the standard is not even good. The banks achieved 63.34 marks, which is a satisfactory standard. In particular, banks should give more emphasis to attaining an excellent score.

- **ICT risk management:** The banking industry, which is heavily reliant on client confidence, is particularly concerned about the security issue [21] This is where ICT risk management enters the picture. It covers Risk governance, Risk assessment, and Risk response which are vital for the existence of any organization. The banks achieved 81.77 marks, which is a very good standard under the BB ICT Security Guidelines. Though the overall situation of our banking industry is not excellent in this regard.

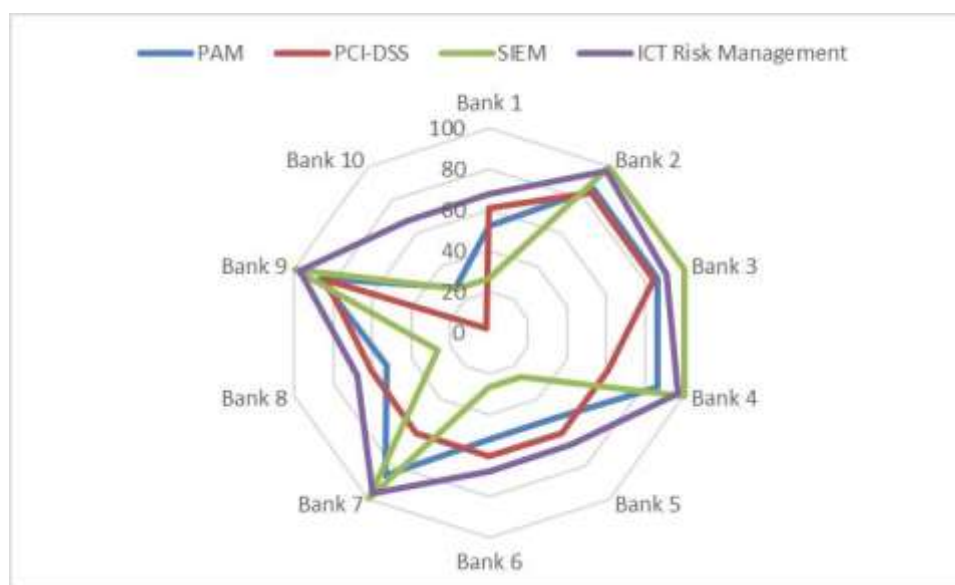


Figure 18. Security Gap Analysis under BB ICT Security Guidelines

6. CONCLUSION

The Bangladeshi banking sector has come a long way in terms of using ICT. Bangladeshi banks have been investing heavily in ICT security measures for years to achieve the security goal. From the customer to the officials, banks are now concerned about all of their protection, including business improvement. There is still a long way to go to achieve the excellence standard of security following the BB ICT security guidelines. Therefore, more study is required in this regard. Future research can be conducted to improve the efficiency of ICT security in order to protect banks

REFERENCES

- [1] Amam Hossain Bagdadee, Argho Moy Maitraya, Ariful Islam, Md.Noor E Alam Siddique, A Review on Hybrid Energy Generation: Cow Dung Biogas, Solar Thermal and Kinetic Energy Integration for Power Production, Energy and Built Environment (EBE), <https://doi.org/10.1016/j.enbenv.2023.09.004>
- [2] Mahedi Hassan, Tuchi Rahman Lata, Nipa Rani, Md. Al- Amin, Md. Al Amin Shak, Likshon mia, Md.Zahidul Islam, Amam Hossain Bagdadee , "IoT-Based Smart Health Monitoring System for Efficient Service in the Medical Sector," International Journal of Engineering Trends and Technology, vol. 71, no. 4, pp. 159-170, 2023. Crossref, <https://doi.org/10.14445/22315381/IJETT-V71I4P215>
- [3] Shahjalal, M.M. Manna Mehedy, Md. Mijanur Rahman, Md. Tuhin Ali, Md. Mosiur Rahman, Amam Hossain Bagdadee; Using microcontroller based solar power system for reliable power supply, Journal of Applied and Advanced Research, 2022, Volume 7: 18-24, Doi: 10.21839/jaar.2022.v7.7550
- [4] Amam Hossain Bagdadee, Zhang, L. Using Static Modulation Power Filter Compensator for Power Quality Improvement in Renewable Energy-Based Smart Micro-Grid System, Lecture Notes in Electrical Engineering, vol 711. Springer, Singapore. 2021, https://doi.org/10.1007/978-981-15-9019-1_104 (Scopus)
- [5] Amam Hossain Bagdadee, SajidAli, Li Zhang, Energy management for the industrial sector in smart grid system, Energy Reports-Elsevier, DOI:10.1016/j.egyr.2020.11.005
- [6] Amam Hossain Bagdadee, Muhammad Yasir Ali Khan, Hong Ding, Jianwei Cao, Yong Ding Li Zhang, Implement industrial super-dynamic voltage recovery equipment for power quality improvement in the industrial sector ,Energy Reports-Elsevier, DOI:10.1016/j.egyr.2020.11.058
- [7] Amam Hossain Bagdadee & Li Zhang, Renewable energy based self-healing scheme in smart grid, Energy Reports -Elsevier, DOI: 10.1016/j.egyr.2019.11.058
- [8] Amam Hossain Bagdadee & Li Zhang, Electrical Power Crisis Solution by the Developing Renewable Energy Based Power Generation Expansion, Energy Reports- Elsevier, DOI: 10.1016/j.egyr.2019.11.106
- [9] Amam Hossain Bagdadee & Li Zhang, Power Quality Impact on the Industrial Sector: A Case Study of Bangladesh, Journal of Electrical Engineering & Technology -Springer, DOI: 10.1007/s42835-019-00220-y

[10] Amam Hossain Bagdadee & Li Zhang, A Brief Assessment of the Energy Sector of Bangladesh, International Journal of Energy Optimization and Engineering DOI: 10.4018/IJEOE.2021010103,

[11] Amam Hossain Bagdadee & Li Zhang, Smart Grid Implementation of the Industrial Sector : A Case of Economic Dispatch, International Journal of Energy Optimization and Engineering DOI: 10.4018/IJEOE.2019100101

[12] Amam Hossain Bagdadee & Li Zhang, A Review of the Smart Grid Concept for Electrical Power System, International Journal of Energy Optimization and Engineering, DOI: 10.4018/IJEOE.2019100105

[13] Amam Hossain Bagdadee & Li Zhang, Power Quality improvement provide Digital Economy by the Smart Grid, IOP Conference Series: Materials Science and Engineering, DOI: 10.1088/1757-899X/561/1/012097

[14] Amam Hossain Bagdadee, Li Zhang & Modaway, Constant & Reliable Power Supply by the Smart Grid Technology in Modern Power System, IOP Conference Series : Materials Science and Engineering, DOI: 10.1088/1757-899X/561/1/012088

[15] Amam Hossain Bagdadee, Li Zhang & Remus, A Brief Review of the IoT-Based Energy Management System in the Smart Industry, Advances in Intelligent Systems and Computing- Springer, DOI: 10.1007/978-981-15-0199-9_38

[16] Amam Hossain Bagdadee, Md Zahirul Hoque, & Li Zhang, IoT Based Wireless Sensor Network for Power Quality Control in Smart Grid, Procedia Computer Science -Elsevier (DOI: 10.1016/j.procs.2020.03.417

[17] Amam Hossain Bagdadee, "Power Quality Analysis by the Ripple Technique" Published <http://dx.doi.org/10.21839> ,Journal of Applied and Advanced Research 2017, 2(4): 227-234

[18] Amam Hossain Bagdadee, "Imitation intellect Techniques Implement for Improving Power Quality in Supply Network Accepted in (Paper Code: IEEE-SCOPE-CUTM-03-16-OR0342) IEEE International conference on Signal Processing, Communication, Power and Embedded System -2016

[19] Amam Hossain Bagdadee "To reduce impact of the variation of power from renewable energy by using super capacitor in Smart grid" Published by World Scientific and Engineering Academy and Society in WSEAS TRANSACTIONS on POWER SYSTEMS Vol.11 2016, USA.

[20] Amam Hossain Bagdadee, Li Zhang, Smart grid: a brief assessment of the smart grid technologies for modern power system, Journal of Engineering Technology, Volume 8, Issue 1, Pages:122-142,2019

[21] [21] Amam Hossain Bagdadee , Md. Bayezid Islam “TO IMPROVE POWER FAILURE AND PROTECT SUSTAINABILITY OF THE ENVIRONMENT IN BANGLADESH BY THE RENEWABLE ENERGY” Published by European Centre for Research Training and Development UK in International Journal of Energy and Environmental Research Vol.3, No.1, pp.29-42, ISSN: 2055-0200, March 2015, UK

[22] Amam Hossain Bagdadee , Nazib Sobhan “Developing model of control stratagem with variable speed drive by synchronous speed in micro-Hydro plant” Published in International Journal of power and Renewable Energy Systems (IJPRES) Vol.2, 2015 PP.88-100 ISSN 2374-376X, USA

[23] Amam Hossain Bagdadee, “ ASSESSMENT OF PV OPERATION IN BANGLADESH Published by European Centre for Research Training and Development UK in International Journal of Energy and Environmental Research Vol.2, No.1, ISSN: 2055-0200, March 2014, UK

[24] [24] Amam Hossain Bagdadee, “Status and Reform towards Development Energy Sector of Bangladesh” Published in European Journal of Advances in Engineering and Technology, Vol.2(2): 24-28 ISSN: 2394 - 658X, 2015, India

[25] Amam Hossain Bagdadee, Abu Salman Shaikat, PROPERTY OF ANCILLARY SERVICES MARKETS ON FREQUENCY CONTROL PERFORMANCE OF POWER SYSTEMS, Published by European Centre for Research Training and Development UK in International Journal of Engineering and Advance Technology Studies Vol.2, No.3, ISSN:2053-5791, 2014, UK

[26] Amam Hossain Bagdadee, Rural Electrification with Renewable Energy Based Village Grids in Bangladesh .Published in International Journal of Scientific & Engineering Research, Volume 5, Issue 10, 1080 ISSN 2229-5518, 2014, India

[27] Amam Hossain Bagdadee, 'Using A Battery Storage Wind / PV Hybrid Power Supply System Based Stand-Alone PSO To Determine The Most Appropriate “Published in American Journal of Engineering Research (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-03, Issue 08, 2014, USA

[28] Amam Hossain Bagdadee, "POWER SYSTEM ANALYSIS OF LOAD FLOW IN RADIAL DISTRIBUTION NETWORK" Published in International Journal of Scientific & Engineering Research, Volume 5, Issue 10, 1080ISSN 2229-5518,2014.India



Md. Saddam Hossain Remus B.Sc. in EEE (IUBAT - International University of Business Agriculture and Technology) Masters in Information Technology (IIT, Jahangirnagar University) Jamuna Bank PLC an IT security professional with the ability to protect organizations from security threats and implement security solutions using various frameworks. Expertise in network security, application security, and incident response. Passionate about lifelong learning with a research interest in the same domain and staying up-to-date on the latest security trends.



Sanzida Akter, BSC in EEE From United International University, MBA From University of Asia Pacific Professional: IT Officer at Jamuna Bank Limited. Information Technology (IT) Professional with 11+ years' experience in managing electronic fund transfer, security patch, encryption, and network server projects. Led Bangladesh Automated Clearing House (BACH I & II) projects and CBS Version Migration resulted in efficient payment processing. With in-depth knowledge and hands-on experience in Banking and Media IT Industry, enthusiastic to expand expertise in Cyber Security e.g., penetration testing, vulnerability scanning, and ethical hacking techniques and enhance my organization's ability to prevent security breaches and protect computer systems and networks from potential threats.



Khaleda Ferdous is an officer at renowned private Bank of Bangladesh. She received a bachelor's degree in Computer Science & Engineering from Institute of Science & Technology of National University Bangladesh, and a Master's degree in Computer Science from Jahangirnagar University, Bangladesh. She received ISO 27001 ISMS certificate from PECB. Currently she is working with IT Compliance, Governance & Security of the bank focusing mostly on the digital security. She is interested in ICT Security Policy making, planning & implementation of particular area to ensure digital security by reducing vulnerability of the digital banking system.