CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY, ISLAMABAD

Evaluation of Factors Affecting the Adoption of Cyber-Security Locks

by

Duaa Ayesha

A thesis submitted in partial fulfillment for the degree of Master of Science

in the

Faculty of Engineering
Department of Mechanical Engineering

2024

In humble reverence and unwavering devotion, I dedicate the entirety of this thesis to Allah Almighty, seeking His divine guidance as I embark on this scholarly journey

CERTIFICATE OF APPROVAL

Evaluation of Factors Affecting the Adoption of Cyber-Security Locks

by

Duaa Ayesha

(MEM213024)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Usama Waleed Qazi	IST, Islamabad
(b)	Internal Examiner	Dr. Mohammad Javed Hyder	CUST, Islamabad
(c)	Supervisor	Dr. Ghulam Asghar	CUST, Islamabad

Dr. Ghulam Asghar
Thesis Supervisor
April, 2024

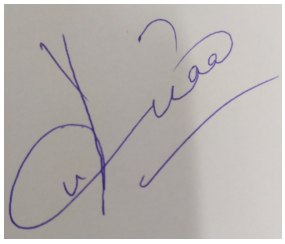
Dr. Muhammad Mahabat Khan
Head
Dept. of Mechanical Engineering
April, 2024

Dr. Imtiaz Ahmad Taj
Dean
Faculty of Engineering
April, 2024

Author's Declaration

I, **Duaa Ayesha** hereby state that my MS thesis titled "**Evaluation of Factors Affecting the Adoption of Cyber-Security Locks**" is my work and has not been submitted previously by me for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/abroad.

At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my MS Degree.



(Duaa Ayesha)

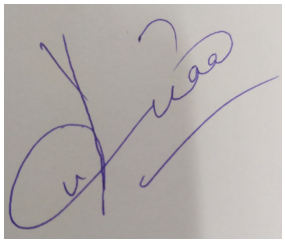
Registration No: MEM213024

Plagiarism Undertaking

I solemnly declare that the research work presented in this thesis titled "**Evaluation of Factors Affecting the Adoption of Cyber-Security Locks**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero-tolerance policy of the HEC and Capital University of Science and Technology towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred to/cited.

I undertake that if I am found guilty of any formal plagiarism in the above-titled thesis even after the award of my MS Degree, the University reserves the right to withdraw/revoke my MS degree and that HEC and the University have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized work.



(Duaa Ayesha)
Registration No: MEM212024

Acknowledgement

In the name of The Omniscient, The Omnipotent, The Omnipresent and The Omnibenevolent for the blessing of choosing me for this endeavor. First and foremost, thank you to my creator ALLAH S.W.T, my life tutor, the most kind, the most generous, ALLAH S.W.T., I owe it all to you, Thank you! I would like to thank my supervisor Dr. Ghulam Asghar for her great effort heartily support and precious time in the completion of my thesis. Under his direction, I fruitfully overcame many complications during my thesis work. In this phase, I am thankful for my parents whose self-sacrificing life and their great exertions and never-ending devotions have permitted me to do my MS Thesis successfully. Thanks to my brothers and friends for their unremitting support, empathetic, and good wishes every time I needed it. Last but not least, I am grateful to all my teachers who facilitated me in every single track of life.

(Duaa Ayesha)

Abstract

Smart cyber-lock technology is considered a well-known idea that has the potential to resolve emergent safety and security matters. This study focuses primarily on the relationship among various factors affecting the adoption of cyber-lock technology. This work analyzes the four factors technical factors, administrative factors, firm size, and technology acceptance model that affect the adoption of cyber-security locks technology. The questionnaire is prepared according to these four factors and distributed among 400 participants, out of which 322 responses are received. Security-sensitive organizations in Rawalpindi and Islamabad are considered as a sample of the population. There are three hypotheses formed through the literature study. Hypothesis testing is performed through different types of statistical tests such as confirmatory factor analysis, reliability analysis, regression analysis, pearson correlation, mediation test through SPSS/AMOS, and moderation test through SPSS/AMOS.

After statistical analysis, it is concluded that all of the factors are significant and their sub-factors have different significant levels separated by categories of highly significant, moderately significant, and significant. Revenues, resources/assets, market Shares, customer demands, capital-labor ratio, productivity, cost, privacy/security, and number of employees all are highly significant. Moderately significant sub-factors are top-level management, effective communication, training programs, awareness campaigns, allocation of adequate resources/budget, and perceived reliability and effectiveness. Resources availability, the culture of an organization, user attitude, potential risks, and vulnerabilities have a significant effect on the adoption of cyber-security locks. so, all hypotheses are accepted after all testing results applied to the data.

Keywords: Administrative factors, technical factors, firm size, technology acceptance model, cyber-locks, cyber security, cyber-locks, Internet of things

Contents

List of Figures

List of Tables

Abbreviations

AF	Administrative Factors
CFA	Confirmatory Factor Analysis
FS	Firm Size
GPS	Global Positioning System
IoT	Internet of Things
PBC	Perceived Behavior Control Management
PU	Perceived Usefulness
R and D	Research and Development
SaaS	Software as a Service
SEM	Structuring Equation Modeling
SPSS	Statistical Package for Social Sciences
TAM	Technology Acceptance Model
TF	Technical Factors
TPB	Theory of Planned Behavior
TRA	Theory of Reasoned Action

Chapter 1

Introduction

1.1 Background

Due to the rapidly changing technology of security devices, everything moves toward secure and organized systems. Smart cyber-lock technology is an eminent concept that can potentially solve emerging last-mile issues. The cyber lock technology was introduced and developed by Videx, Inc. in the USA, which is also the pioneer in the data collection and identification process. In 1979 the designing and manufacturing process of innovative electronics was founded in Corvallis. After that in 1985, Videx, Inc. introduced the first portable bar code scanner, and additional RFID tag technology was added up with a small difference.

The cyber lock technology was founded in 2000 when Videx, Inc. first electronic lock and smart keys were openly offered at the market level [1]. In 2013, Cyber-Lock emerged as an independent company by introducing a strong design of the technology that continuously worked on future innovations. Cyber-locks became an independent entity and developed relationships with different technologies by sustaining them internationally. It functions by integrating the scheme with the support of an organization and maintains a high level of security system.

Cyber-lock is the symbol of safety and security; nowadays, it is transformed into a valuable product. After this lock installation, the customer experience has increased visibility in terms of convenience. Cyber-lock is known as key-centric

access considered for increasing security, safety, liability, and key control of the system [2]. Based on the design of programmable smart keys, cyberlock resolves security-related difficulties that no other scheme has offered in recent years. There are different benefits due to which it is applied and used in security-sensitive organizations. It is versatile and full access is gained; only rechargeable batteries charge the keys by replacing the old cabling system, which is cost-effective. There is a superior key control that is programmed through the access permissions for authorization of individual users. In case the key is lost, it can be easily removed from the system by deactivating it from the system and all connected means could be stopped from the access point.

High-security locks are operated through an information exchange process and regulate the authorization for users. Both key and lock access events are declared in the software and unauthorized access attempts and access could be granted and managed through cyber-link software only.

Figure 1.1 shows a schematic view of the cyber-locks used in different organizations.

FIGURE 1.1: Schematic View of the Cyber-locks

The audit trail is gathered and presented with the communication device, so all activity data is downloaded with new access privileges. The electronic key is programmed through access to privileges, in which each user is present in the list of locks. The programming is performed in a way that the expiring date is managed to increase the security concerns for the locks. The audit trail is viewed through cyber audit software related to management and customized periodic notifications

over suspicious activities. The reports are generated automatically and after that complete events are monitored and evaluated properly based on the data.

Cyber-security locks technology is in the spotlight and entails extensive research due to its advanced role in various fields [3]. Whereas, the cyber-security locks influential factors adoption in security-sensitive organizations is not much focused in the past. The adoption of cyber security locks technology is an overlooked issue in literature and it should be explored because this technology can increase security concerns. Additionally, in the past, very little research has been directed towards the relationship between cyber-lock adoption and security management. Therefore, this study will try to address and evaluate issues in an organization related to the adoption of cyber-security locks in Pakistan. Moreover, this work also interlinks the two main fields; information technology and project management to examine different aspects of security and control.

Four main variables (firm size, technical factors, administrative factors, and technology acceptance model) are explored in this research work as influential variables in the adoption of cyber-locks technology.

In this research study, technical factors act as an independent factor and the dependent factor is the administrative factor, which is further divided into subfactors for more clarity of the concept. The technology acceptance model acts as a moderator between technical and administrative factors of an organization that is analyzed through the user behavior towards technology. The firm size is used as a mediator between technical and administrative factors. The collective analysis of these four factors will be conducted to explore and identify those parameters that significantly contribute to cyber-lock adoption.

The technical factors in the adoption of advanced technology act as vital roles that belong to privacy and security details. Technical costs and potential risks also belong to the operability and efficiency of the technology. Administrative factors are related to managing functions of the technology through both internal and external management of an organization's affairs. Allocation of adequate resources related to technology adoption is performed by top-level management.

Effective communication is accomplished through training programs and awareness campaigns due to which the benefits of technology are also evaluated. Firm size is related to different measurements such as sales, total assets, revenues, productivity, market value equity, and number of employees in an organization. Firm size is explained through different schemes and methodologies by past authors in their study but in our study, it is considered as a mediator for technology adoption processes. User behavior assumes the acceptance of technology through user (employees and consumers) intention and is resolute by the usefulness of technology in an organization. Through TAM user behavior is distinct in our study with a framework that advances technology understandings in two ways by accepting the technology and after that adopting it suitably over an organization.

1.2 Problem Statement

The smart lock occurs in a fluid phase with neither dominant implementation nor much adoption in underdeveloped countries, especially Pakistan. Recently, cyber-lock technology adoption has been comparatively very low. Researchers highlight the design and implementation of cyber-locks to a large extent; however, the adoption or reception with an interrelationship among variables is shaded and not addressed in the literature as much for profound consideration. Technical and administrative factors are explained in past work composedly and separately but other factors linked with it are not addressed in past studies.

This research highlighted the influential acceptance variables of cyber-security locks technology and interrelationships to contribute with a systematic approach. Therefore, this study will try to address and evaluate influential factors related to adopting cyber-security locks in Pakistan. Moreover, this work also interlinks the two main fields; information technology and project management to examine different aspects of security control and new technology adoption management.

1.3 Research Questions

The following are the research questions for this study:

- **Research Question 1**

What are the influential variables in the adoption of cyber-security lock technology over an organization?

- **Research Question 2**

What is the association of variables among administrative factors, technical factors, firm size, and technology acceptance model in the adoption of cyber-security locks technology?

- **Research Question 3**

What is the apparent usefulness of the adoption of cyber-security locks technology in the framework of Pakistan?

1.4 Study Objectives

The main aim of this study is to analyze and identify the critical factors, which play an important role in the adoption of cyber-lock technology. This work has specific objectives described further down:

- **Research Objective 1**

To explore and identify the key adoption variables for the adoption of cyber-lock technology in an organization.

- **Research Objective 2**

To examine the association among administrative factors, technical factors, firm size, and technology acceptance model in the adoption of cyber-lock technology.

- **Research Objective 3**

Testing of research model variables for adoption of cyber-security locks in the framework of Pakistan.

1.5 Significance of the Study

In this era of technology, almost every business and organization gets a competitive advantage through the use of advanced technology concerns. This research will be supportive not only to the applicability context in the field of cyber security but it will also provide solid suggestions that security can be increased by the adoption of cyber lock systems in an organization. This research will reveal the various aspects of advancements related to cyber-lock systems adoption in organizations. It will also help to understand the hurdles and reasons behind the reluctant behavior towards the adoption of cyber lock systems in underdeveloped countries and illustrate the potential benefits associated with the adoption.

The analysis would reveal why this is the best time for organizations to implement cyber-locks as their business solution. This study will help the organization that how cyber-locks can be managed through the use of different security solutions with advanced means. Better understanding could be developed and this domain in particular has not been investigated in under-developed countries, so this study will be good input in the field of cyber-security locks management. The existing research gap in previous literature is fulfilled because research on cyber-lock adoption variables has not been explored yet in the field of cyber-security for different countries, especially in Pakistan.

1.6 Thesis Organization

The road map of the complete research work is described sequentially through a short overview of all chapters given below.

- **Chapter 1**

This chapter is an outline of the complete research work in which the research background, problem statement, research questions, objectives, significance, and supporting theories of the study are explained.

- **Chapter 2**

In this chapter, the literature is covered related to the previous work done on this topic. The scholarly knowledge described in this portion includes past work, research papers, journals, books, and annual reports. All of the related material of cyber-locks and adoption factors in an organization is defined in this section properly. Different theories are linked with our work so, all of them are highlighted in it. Shortly, in this chapter all of the past research work related to the thesis topic is covered properly.

- **Chapter 3**

Chapter 3 is all about the methods and procedures that are used in the research work to conclude the results. Through the primary data collection process, the analysis is performed by structural equation modeling. After that systematic technique is used to analyze the outcome of the complete study, and the execution is performed at the end. The complete details of the study with design, hypothesis, questionnaire, and results are provided in this portion.

- **Chapter 4**

This chapter is an analysis of the results that are obtained through questionnaire data in the previous chapter. Different statistical methods and testing techniques are used for data analysis. All types of testing results are discussed with critique and after that, the hypotheses acceptance and rejection decision is also highlighted. A clear and well-structural analysis of results is categorized that provides a sketch of the outcomes and significance linked to the concerned field.

- **Chapter 5**

In this chapter, the conclusions are drawn based on the detailed analysis. Derived conclusions explain the complete findings with limitations and implications given out appropriately. The discussion is transparent and sufficient enough to define the complete view of the research study. The recommendations of the study are documented along with the future direction.

Chapter 2

Literature Review

This literature review section is focused on past academic research papers, which provide new arguments and insights. Literature work is organized into six main sections discussing different past studies. The first section is "Cyber-security locks adoption in modernization", the second section is related to "Firm size and adoption of technology", the third section is "Technical variables and adoption of technology" and the fourth section is "Administrative variables and adoption of technology". All these sections are divided into sub-factors based on the literature. The fifth section is related to "Theories of technology adoption and their integration" All of these sections are explained through past research work.

2.1 Smart Cyber-Locks Adoption in Modernization

Smart cyber-locks are used for different applications to enhance the security and safety of an organization. The smart cyber-lock software allows assigning keys, setting expirations, audit trails, access schedules, and generating custom audit reports. Easy access is provided through web browsers on smartphones, laptops, tablets, and desktops for smart monitoring. The system is managed through administrators and customized access is provided to every individual connected to the cyber-lock. This technology makes smart monitoring and evaluation of

personal assets and sites easier with high scientific reliability and management processes.

In an advanced research work by duaa et al., [4] cyber-security locks are integrated with SCADA (Supervisory Control And Data Acquisition) software for the process of smart surveillance management. The main goal of this work is to provide an efficient system in terms of security and safety to solve emerging monitoring and management issues. Different site data is collected in this work to analyze issues that are resolved after the synchronization of cyber-locks with SCADA software. After synchronization of SCADA with cyber-locks smart monitoring and evaluation are performed through which security is managed to some extent. Attempts of user premises access, cyber-attacks, and human errors are reduced and site data is monitored properly with audit reports and evidence. The results of before and after synchronization in cyber-security locks and SCADA are shown in figure 2.1

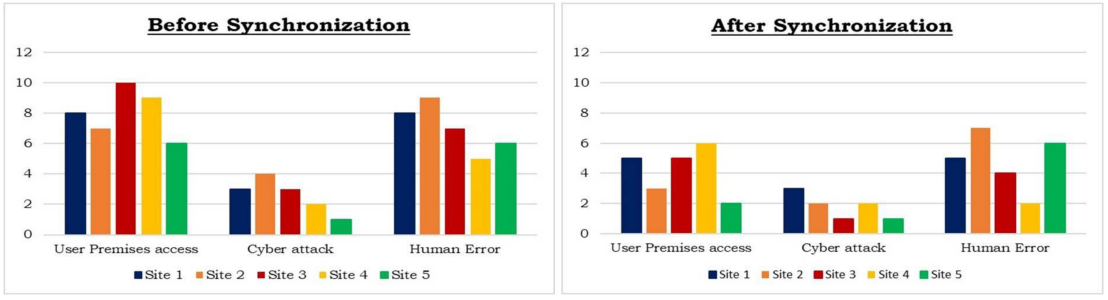


FIGURE 2.1: Comparison of Results Before and After Synchronization

Zhang et al [5] reported work on the intelligent door lock system with face recognition, in which the Linux platform is used with Raspberry Pi. The system is designed by integrating Android and Java Enterprise Edition, to scan out the data. A person's face data is recognized through input interfaces of a Raspberry Pi camera installed in the door lock. The input number or pass-code is set by the system's administrator and data is managed through mobile devices as well as from the computer system.

Cyber-locks are introduced in a research work based on London urban areas and the main concept is smart locks and smart customers. The survey is conducted for London's urban areas in which different barriers and drivers are identified through stakeholders' interviews. The potential communication channels among

customers are formed, which results in new opportunities and creative solutions for upgraded models of cyber-locks [6]. Three types of analysis frameworks are formed such as Rogers's diffusion of innovation, the chasm model, and factors affecting the diffusion of technology to analyze smart cyber-locks. Figure 2.2 highlighted options indication with yellow (neutral), green (good), and red(problematic) categories in cyber-lock adoption, respectively.

Rogers Diffusion of Innovation	The Chasm Model	Factors Affecting Diffusion of Technology
Relative Advantage	The Market Segment	Improvements of Inventios after First Introduction
Compatibility	The Product Offering	Technical Skills Among Users
Complexity	The Competition	Skills in Machine-Making
Trialability	Distribution and Pricing	Complementaries
Observability		Improvements in Old Technology

FIGURE 2.2: Three Model's Technology Adoption Frameworks

Smart locks are dedicated to technical solutions for parcel delivery obstacles. Innovations in cyber-locks for the delivery process potentially reduce the costs and enhance the sustainability for receiver satisfaction. This study survey determined that users are mostly hesitant to adopt cyber-locks in the delivery process just due to security concerns. This research is related to the failed delivery of online purchases that occurred due to the door-unlocking process at delivery time. In this work, the challenges and opportunities of home delivery practice and unnecessary logistics costs are explained from the consumers' perspectives [7].

Another research work Xin et al., [8] is conducted to explain the smart cyber lock mechanisms in attribute-based access control (AAC) for hotel visitor identification. The identity of visitors is verified through encryption and a cascading delete function scheme that is used to improve the applicability in complex situations. An administrator of the system modifies the policy directly and prevents users from unauthorized access through the cancellation of access. In the case of a malicious user attack, the smart cyber lock will be revoked and users will be analyzed through Bluetooth low energy (BLE) authentication and pairing process.

Hassani and Raihana [9] discussed the security evaluation related to smart-lock systems. They identified that the cyber-lock systems are relatively secure with only

a few weak areas like DoS (Denial-of-service) attacks, erratic password policy, and cloning for locking/unlocking of smart locks in the information-gaining process. Existing security flaws in today's society are evaluated and the contributions of smart lock systems, especially in IoT product development are analyzed in this research. Attempts of attacks can be identified through penetration testing and threat modeling.

An Android application is developed for smart lock system control and other IoT-connected appliances in the home are properly managed. The users can lock and unlock the smart lock anywhere in the globe with features that include revoking and granting access to the system. Through the hardware and software integration process, IoT smart locks are promoted with the smart home concept. The attributes are set that include event date, event location, and fine-granted control to access the cyber-locks [10].

Cyber technology is described as the locks control system that is managed through mobile devices as well as from the computer system. Bluetooth technology has low power and makes the system more reliable with all gadgets so, this is used in these smart locks study. Due to the special features of Bluetooth in the design of the system, the comfort and security of the users are increased. This lock system has been implemented through IoT development as it opens and closes through password and gadget control of the user [11].

Jeong J. [12] analyzed the IoT-enabled door lock systems in ATMs (Automated teller machines) and vending machines with unmanned automation. Cyber locks are introduced that are used for automation and have different concerns applied through advanced terms and conditions. This research projected the smart door lock system development strategies for authentication with detailed event actions. Data is received from the sensors of the lock and proper file log management is generated to avoid the forgery of vulnerable hacking alarms with improved security issues.

The blockchain smart door lock system is designed to improve security and safety issues to a large extent. Data probity and non-repudiation are provided in this system by both host and guest globally to manage the complete blockchain of an

organization. Cyber-security locks become centralized with vendor and pin-pad to provide remote access management process. This work proposes a new feature in which guests have explicit approval and cease the lock access during their stay in the hotel. The cost of system design for the Ethereum blockchain is low, users are only charged fees in terms of an action performed on the blockchain [13].

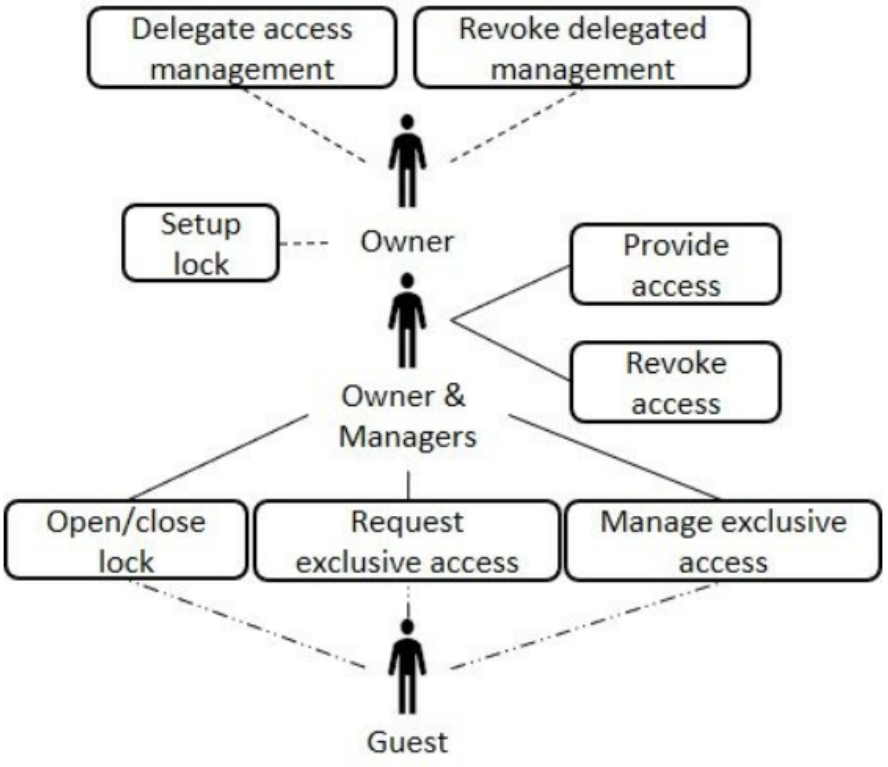


FIGURE 2.3: IoT and Blockchain for Smart Door Lock System

In another research work, Fichtner [14] properly explained cyber-security by conceiving different mapping approaches. Common approaches are analyzed as the structural components that have different roles justified by economic order, privacy, and security. The custom audit reports are generated and mailed to the concerned person after every key event performed on it. An analysis is performed with fundamental components prioritized by cyber-security such as referent object, threat, scrutinizing actor, and security response that distinguish problematic areas.

The futility of cyber security locks for different university campus crimes is analyzed. Card reader locks are installed in the campus building and it is analyzed that the locks reduce the crimes within the campus significantly. The crimes become limited in different campuses as unauthorized people do not enter easily and

approach the target. In this research work, 452 private and public universities data are evaluated. Card reader locks strengthened the security protocol in the universities and fewer crimes occurred in cyber-technology campuses as compared to those campuses without cyber technology [15].

Pevalic et al., [16] described the prototype of IoT and GPS-enabled smart door lock systems to secure the users. The system is designed and tested with a 10-meter threshold of the user's distance from the pre-determined location captured in the Android application. The data is received with GPS coordinates and the host makes the system enable or disable with the user's proximity and controls. Customized access is provided to key holders only and schedule expiration is managed weekly to improve security terms. The proposed system provides security functions that transfer all illegal attempts with recorded images to authorized mobile devices of the users. The alarm works when a physical damage sensation occurs in the door locks for remotely operating devices. The data is sent to the cloud server and the activities are managed for unmanned venues. This work improves cyber-lock efficiency, tracking accuracy, and the quality of the mobile application.

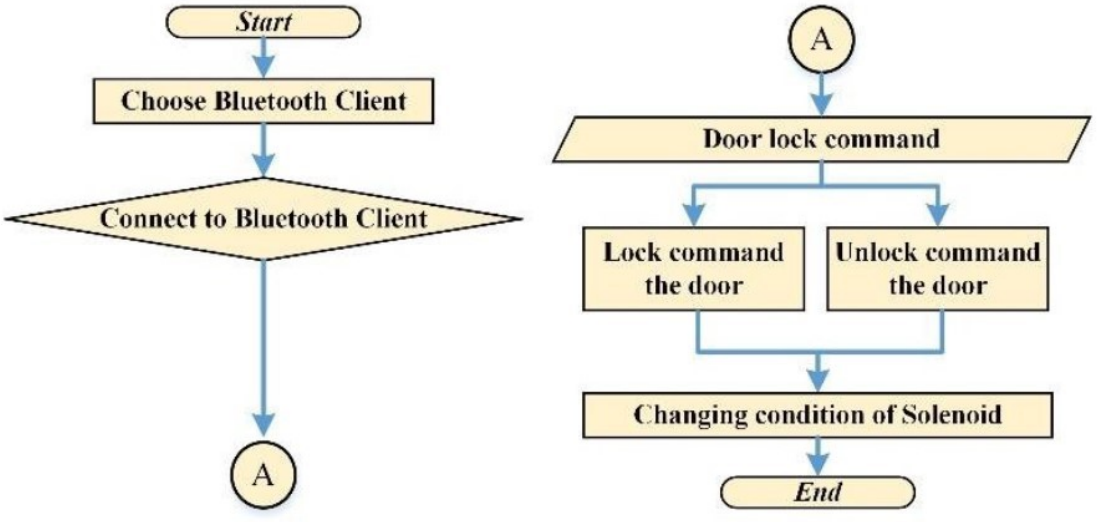


FIGURE 2.4: GPS-Enabled Smart Door Lock System

The configurable intelligent security system is evaluated by Das [17] and it is managed through a 3F (three-factor authentication) smart lock system. Three-factor authentication is applied that is configurable and makes an additional security layer in the system. Through this authentication process, one-time password

(OTP) verification is performed after that it is manipulated according to biometrics, and GPS voice-enabled technologies. The proposed model of this work is economical and has end-to-end security for the users to maintain the complete integrity of the system.

IoT smart door lock device (IoT-SDL) development is proposed by Derbali [18] with a secure system that can unlock the door without any physical connection of a key. Internet connectivity is needed for this system only; therefore, the name and password of the home Wi-Fi are inserted in Raspberry Pi. The control of IoT-SDL is possible through a web browser and the function of two-factor authentication is required to unlock the door. Different approaches and tools are used in this study such as functional and non-functional requirements, operating principles, and software components that make door access smarter in system models.

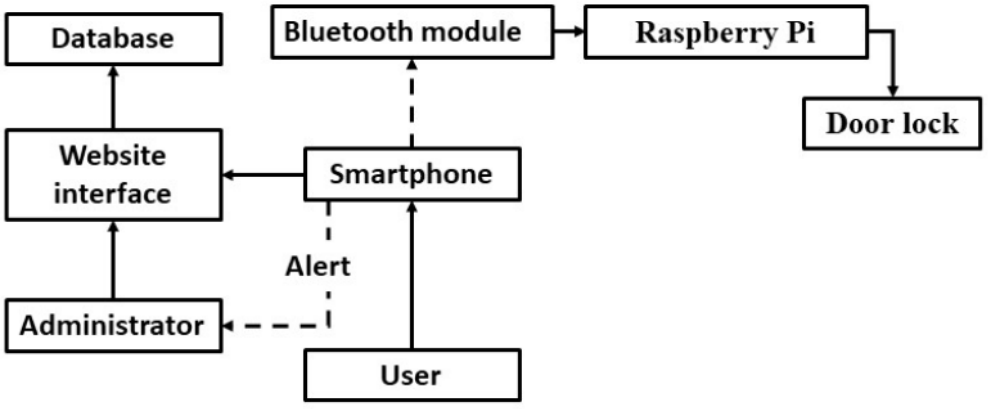


FIGURE 2.5: IoT Smart Door Lock Device (IoT-SDL) with Raspberry Pi

2.2 Firm Size and Adoption of Technology

Firm size is a crucial factor for the acceptance of new technology in an organization. The firm size is decided and utilized based on different sub-categories. It measures market value, total sales, total assets, profitability, corporate leverage, and others. The firm size in technology acceptance requires capital investment and human resources for the complete utilization of company assets and resources.

According to the research work of Aldieri and Fenci [19] empirical and theoretical analyses should be done for sustainable innovation and firm size. Technological

innovations in firms require more skilled employees for the long run, which increases the budget as well as challenges for an organization with its work-structure. Smaller organizations find it more challenging to implement and preserve new technology as compared to larger organizations. On the other hand, innovation adoption is compulsory with a mediating role in terms of sustainability as it minimizes the cost of production and creates future opportunities. The internal and external effects of innovation are explored that impact the firm size in technology adoption.

Oliveira and Martins [20] assessed information technology adoption with the empirical literature on firm competitiveness and enhancement of the country's economy. Determinants of IT adoption have a vital effect on the research model in provisions of firm productivity. Larger organizations are expected to have devoted IT departments to manage new technology activities. IT innovations depend upon three main attributes such as organizational readiness, perceived benefits, and external pressures in the technology adoption process. The comparison is performed on the IT adoption model for individual level and firm levels through innovation in technology, organization, and environment (TOE) theories' frameworks.

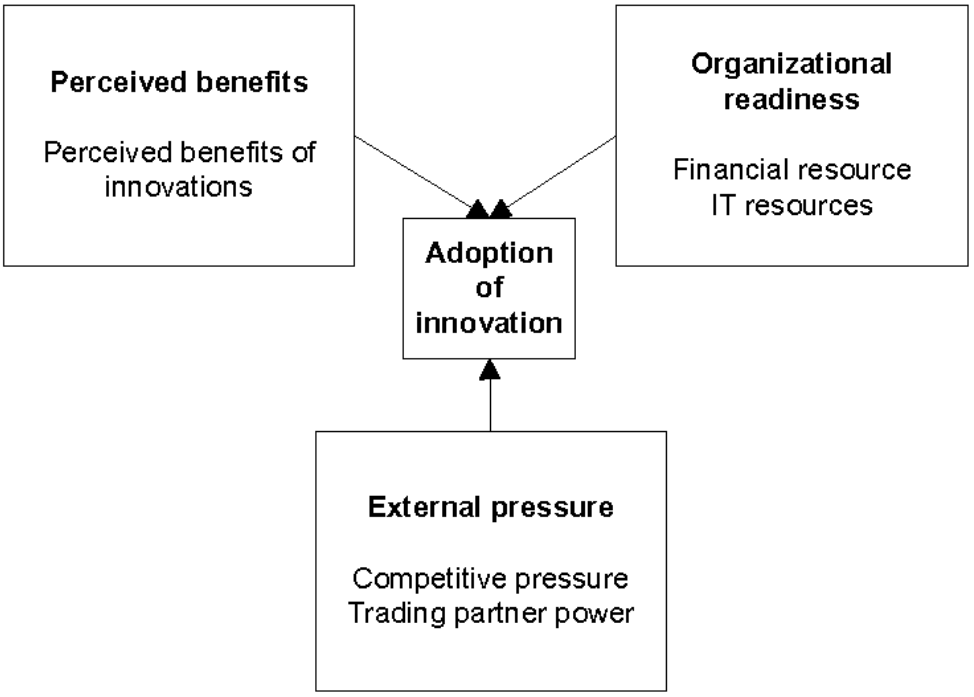


FIGURE 2.6: Information Technology Adoption Model at Firm Level

The structure of an organization is related to the firm size and it is considered essential due to the mediating role of management in technological changes. It is found that the firm size is considered to be an essential predictor in technology adoption and vigilance of new strategies. Through variance analysis, the internal factors of technology adoption are separated and compared with the principal components of the firm. This work explains the relative study of firm size through which the technology adoption is formulated [21].

Financial performance and environmental innovation vary suggestively with the firm size and complete engagement is required with positive effects. Larger firms benefit from environmental innovation with their codes of conduct while the smaller firms grow with the response and demand of the customers. Andries and Stepha [22] explained that the firm co-relation and importance are related in terms of firm performance and environmental innovation. It is clear from this research work that environmental innovation mediates positively with firm performance.

Lin et al., [23] studied the automobile sector firm size that is analyzed by GIS (green innovation strategy) and CFP (corporate financial performance). Customer pressure, government pressure/change, technology changes, market change, and environmental/financial performance are linked directly with the co-relation of GIS. Small firms need high GIS investments as compared to large firms' size due to variation, visibility, and better resource access to generate high profits. The empirical results indicate that CFP and GIS positively affect each other and the firm size negatively moderates both.

Hirdinis's [24] investigated the firm size with capital structure on the firm value that is moderated through the profitability of an organization. The analysis shows that capital structure has a negative effect on firm value. The firm size affects an organizational ability to handle potential customer demands and market fluctuations. The profitability of an organization has no vital and significant effect on the firm value and does not mediate the relationship between capital structure and the firm value. Overall, this research shows that the profitability of any firm externally affects both firm value and capital structure and the firms with high profitability adopt technology in a significant manner.

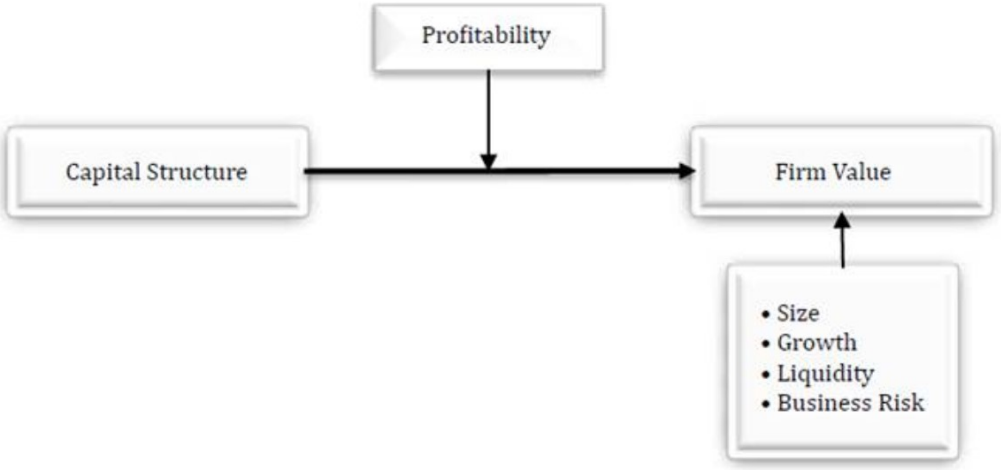


FIGURE 2.7: Capital Structure Firm Value and Profitability

To promote high-technology applications and innovation, it is compulsory to increase business activities at a higher level. The ability of the firm is hindered by relying only on resources. This research explained determinants related to the firm size that include wage, number of employees, employees' age, market position, international trade, and business performance. In small and middle-sized firms, the average wage per employee and employee age of any firm are linked negatively with firm performance. Furthermore, a high global value chain and better international market promote high technologies in firms that pay better to the worker for their high skills [25].

Company size and profitability variables are linked directly to internal leverage and are empirically affected by technology adoption. The factors in technology adoption include company size, corporate leverage, financial performance, and profitability. From the findings, it is inferred that larger firms have high technology adoption due to better financial statements, high profitability, more technology knowledge, and advanced information systems as compared to small-size firms [26].

Kwon et al., [27] analyzed the firm productivity, which is selected from the firm size in adoption of technology. The production function is applied that involves capital and total labor for technology adoption process influence. Different process technologies are applied to the given set of data and verify the degree of analysis. The results indicate a positive effect of technology adoption on the firm's

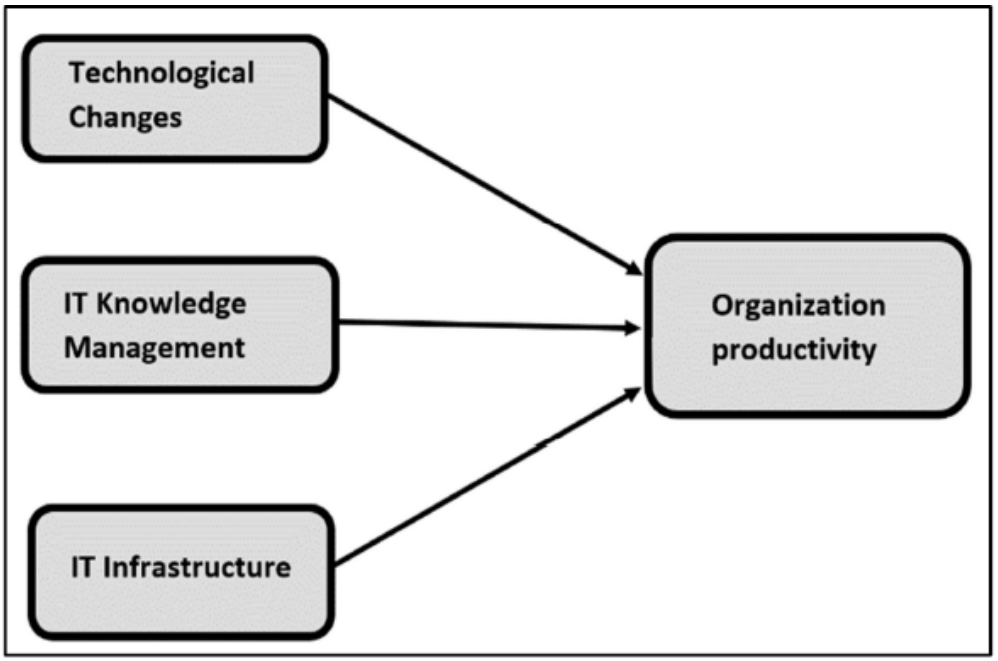


FIGURE 2.8: Firm Productivity Factors in Technology Adoption

productivity/output. It also explores the effect of technology acceptance both theoretically and empirically on the firm's productivity.

Lakhwani et al. [28] studied factors that are related to the change in the firm's productivity for IT knowledge management and organizational infrastructure. Managers are linked directly to organizational productivity and resolve issues in the adoption of technology. IT knowledge management is involved in the decision-making process and investment so, it is considered important for firm productivity. In other terms, productivity is based on employee observation and technological adoption towards personal aspects. Both profit and non-profit firms are affected in different ways for productivity after new technology adoption. Further analysis exhibits that R and D (Research and Development) funds, managerial factors, employee productivity, and capital-labor ratio are important in technology adoption.

Top management must have high technology knowledge with top priority for new technology adoption because it increases productivity. The impact on firms' productivity should be analyzed with their estimation of technology adoption. The structural model is provided in this work-study and managerial implications are also considered with several contributions to analyze the adoption effect on firm size. It is more challenging to implement and maintain new technology in smaller

organizations. If the technology is accepted by everyone (top to low level) in a significant and positive way, productivity is improved otherwise it shows a negative impact on an organization [29].

Opportunities are maximized with the technology adoption process and the development of an inter-firm learning process. Adoption depends upon capital-labor ratio and urbanization, as large organizations adopt technology in a faster manner as compared to small organizations. Adopters in the firm adopt new technologies that gain gross profit and reduce the cost of acquisition-related to an organization's characteristics. The cost of technology adoption varies with firm size as the diversity of industries for different firm attributes [30].

2.3 Technical Variables in Technology Adoption

Technical factors provide substantial, immersive experiences and qualities that lead toward the operation of an organization. Technical factors affect sales, competitors, suppliers, and customers in direct or indirect ways for complete operation processes. Technical factors are technological means that include communication resources, production techniques, information technology, marketing, logistics, and new methods applied for improvement in an organization.

Privacy and security are considered salient features in any organization for the adoption of new technology by every individual. Contextual relationships are important in privacy-related adoption factors as they are connected with the present and future management of an organization. Knight et al., [31] explored privacy and security apprehensions in the adoption of technology especially by older adults of an organization with an informative notion. In this work, the APCO (antecedents, privacy concerns, and outcomes) model is used with arguments upon different findings and proposes an expansion related to privacy outcomes.

Data security is very important in the technology adoption of digital tools, smart schools, and many others. After an analysis, it is indicated that the privacy security chasm leads toward technology adoption. Privacy speech become a barrier in most of the education sectors due to data protection and risk issues other

than the lack of resources availability issue. The problematic factors related to privacy in the education sector for technology adoption are identified. Educational technology adoption takes a long time decision with consequences for both students as well as society [32].

The adoption of new technology increases every day due to the demand for data protection, information privacy, and safeguarding of stakeholders' data for privacy-enhancing technologies (PETs). After the implementation of PETs, compliance is ensured with regulations and customers' trust in an organization. Technical factors are highlighted in technology acceptance and its effect on an organization's outcomes in the form of performance. Through the TOE (technological, organizational, and environmental) model, the PETs should evaluate the managerial readiness, size, and market performance of an organization. The technical factors found in technology adoption are cyber security awareness, perceived benefits, cost, and IT infrastructure [33].

The research conducted by Liu et al. [34] is also related to technical training in the acceptance of new technology with a case study of low-carbon and fertilization technology practices in China. Businesses have faced more pressure in competition to the adoption of advanced technologies especially in terms of organization performance, culture commitment, and internal market. The strategic value in technology adoption is large by the managerial department as compared to technical departments. This study also examines the effect of technical training on management practices for the adoption of advanced technologies. It is hypothesized through logistic regression that education and technical training facilitate technology adoption and promote it to a larger extent. Some companies are in the routinizing phase and less over the infusion phase and hence, adoption is not more reliable.

Nambisan and Wang [35] highlighted barriers that are linked to technology adoption in different technical web-based applications. Technical barriers occurred due to a lack of knowledge, security standards, and set-up costs of hardware and software. Barriers occurred in web technology because this is not yet mature enough so alternative technological solutions are challenging in this era due to privacy.

The perceived reliability and efficiency of technology impact their adoption. Lack of resources, complexities, and technology utilization has also become an issue for both financial and human-functional rations in web-based technology adoption.

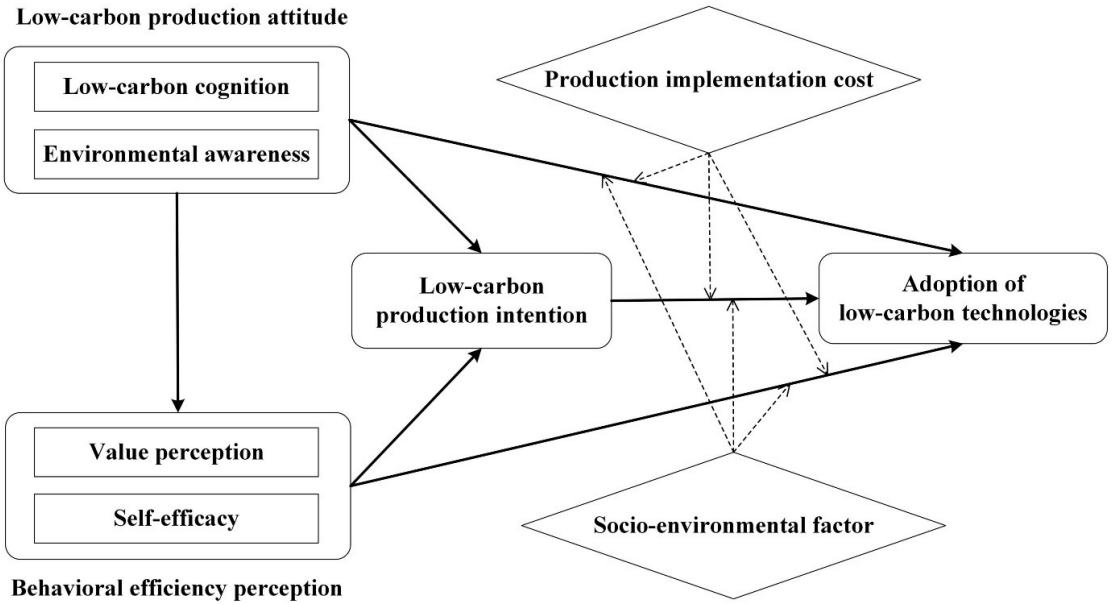


FIGURE 2.9: Adoption Factors of Low-Carbon and Fertilization Technology Practices

Andersson et al., [36] identified the technology adoption changes that occurred with time-to-time advancements; therefore, new technology concepts should be clarified at the individual level of users. The technical adoption factors are analyzed through employee training, technology compatibility, and resource availability in an organization related to new technology. In this work, three main technical variables are highlighted that are co-related with each other such as knowledge, innovation, and technology. Innovative ideas are important in every phase as they increase technology knowledge, which is helpful in technology adoption.

Due to the uncertainty in technical investments, the management and operational transition are not highly prioritized. The security and safety management model explains how the capability of event responses is improved and accidents are lessened. Security management investment is cost-effective, which is also proved in this work. Factors of security and safety risk management are analyzed because of new technology adoption. The easiness in operability of new technology affects their adoption in an organization. Existing systems have an operational transition as well as vulnerability change, which investigates the controlling processes in the

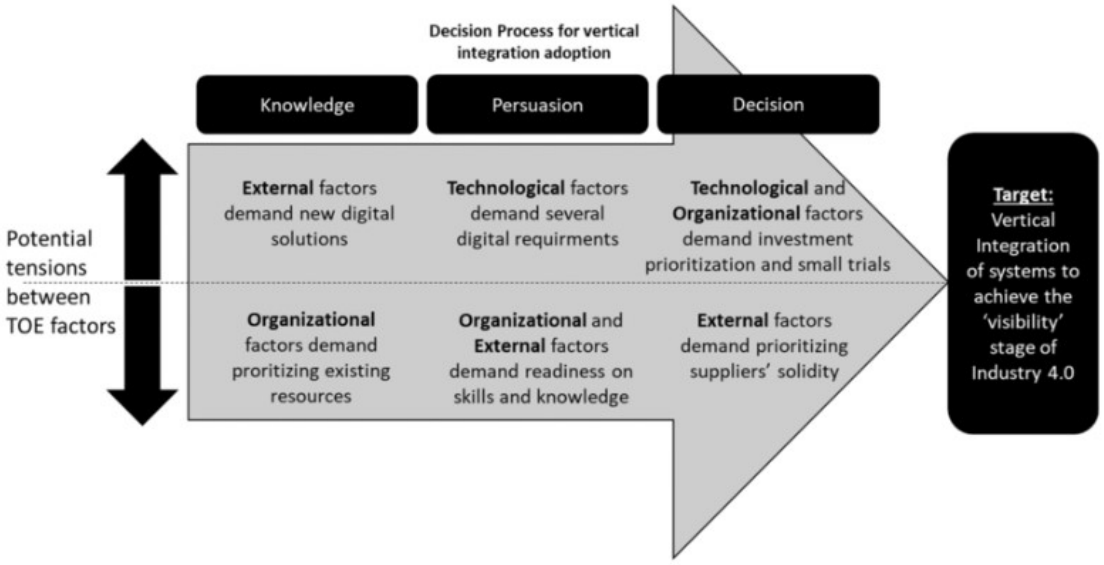


FIGURE 2.10: Different Organizational Factors in Industry 4.0 Adoption

adoption of advanced technology. The Norwegian oil and gas industry is taken as an example of a dynamic system model [37].

Organizations that spend time on the technology adoption process also need to invest money and time in training to build technical skills among employees. Due to this compatibility, technology productivity is gained and performance is increased. Boothby et al. [38] analyzed the technical factors as an independent factor in terms of technology training, functionality, easiness, and productivity performance of an organization. It works on a strategy of combination, in which technology and training utilize the adoption process and enhance the economic performance of an organization.

Ogata et al. [39] analyzed the production risk and technology adoption roles through an empirical study, especially in crop failure. Risk factor analysis is essential in assessing the new technology adoption processes because they are linked directly to a farmer's production processes. Agricultural innovation is important as it improves production and attracts farmers for technology adoption. The magnitude and direction of farms affect the technology adoption process that is addressed in this work.

Janssen et al. [40] explained blockchain technology and analyzed the technology adoption relation with three factors that are institutional, technical, and market

fluctuation. The majority focus of this work is to analyze technicalities in the adoption of technology through a conceptual framework. The proposed framework is used as a reference point in blockchain adoption as it can refine, expand, and evaluate organizational requirements. Blockchain technology framework represents that market, institutional, and technical factors correlate and mutually influence each other.

In the study reported by Berlilana et al. [41] organizational benefits are analyzed in security adoption processes with cyber security and cyber readiness. Data is collected from different organizations and after that cyber security and their performance impacts are evaluated. This work integrates a framework based on cyber-security efficiency and readiness that examines different factors' performance for the adoption of organizational security with tangible and intangible benefits. It is communicated that cyber-security readiness positively impacts security performance and improves social support accountability.

Organizations that set their resources every year for new technology adoption do not face difficulties and productivity is improved as compared to their competitors in the marketplace. Jiao et al., [42] examined the effects of resource availability in technology adoption and their effects on stakeholder pressure and managerial observations. This conceptual model is formed and the results reveal that resource availability significantly impacts the technology adoption process. It also indicates that the relationship between the availability of resources and technology adoption is mediated partially.

This is the first step towards the security tool adoption linked with the diffusion of innovation theory. Theoretical justification of factors is used in this work to analyze the influence of developers in the process of decision-making for the adoption of new secure technology. The compatibility of new technology with different operating structures and stages affects their adoption. This research work is related to independent technical and personal factors, which are influenced by the adoption of new secure technology. To write more secure code, security tools are used by software developers in their programs for an analysis process [43].

Privacy and safety issues over personal perspective are more imperative in the new technology adoption model. Thus, knowledge and training about technology are important to satisfy every individual in an organization. This study emphasizes on critical assessment of technology adoption for the diffusion process of information technology, which is continuously updated and examined carefully with old and new apprehensions and resources. Diffusion patterns in the adoption of technology vary with different types of information systems in an organization. It is discovered that the diffusion process makes relationships effective and efficient with increased productivity [44].

Personnel capabilities, management capabilities, and infrastructure capabilities are linked to an awareness of technology adoption processes. Employees and the general public must be aware of the security risks and mitigation plans because information assurance has more association with cyber security compliance. The relationship between cyber security compliance and the technology adoption process is explored through the planned model. Technical and social systems ensure security measures and independently control the organization's information system. The designed model of this work assessed the factors and their impact on compliance of cyber security of an organization to improve the vulnerable terms [45].

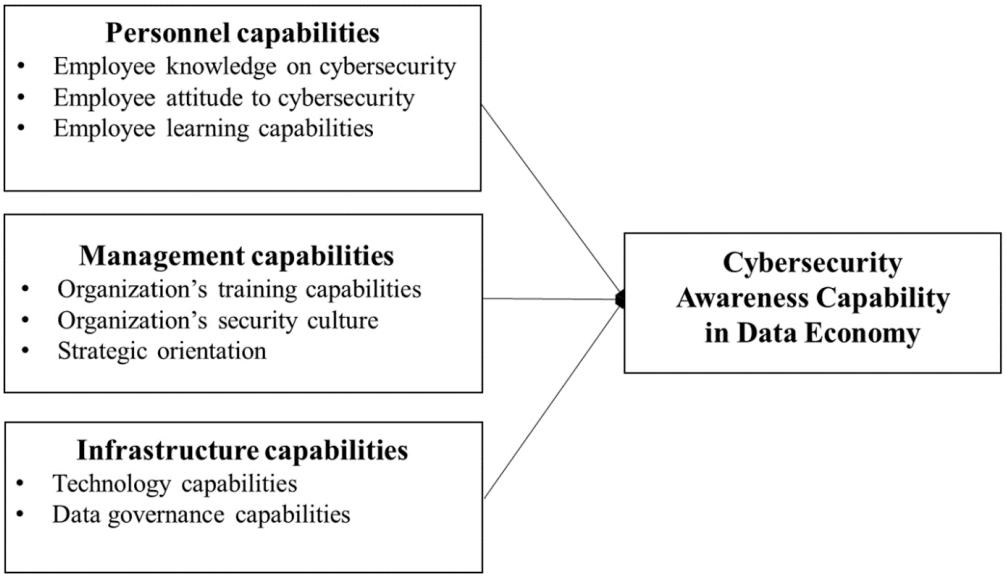


FIGURE 2.11: Cyber Security Awareness in Technology Adoption

2.4 Administration Factors in Technology Adoption

Administrative factors may be external and or internal depending upon the involvement of an organization's structure. Leadership communication, recruitment, decision-making process, supervision, line of authority, and innovation concepts are the main determinants of these factors. The structure of an organization has a hierarchical arrangement, which outlines the authority to determine the roles, responsibilities, and power that are assigned for work process flow at management levels.

Managerial involvement is considered the key adopter in IT innovation and characteristics applied in different patterns. In many of the previous studies, the awareness aspects are still environment-dependent and inconsistent; therefore, the aim is to analyze the depth and discover some characteristics such as economic, technical, information, and external. Technology awareness, security policies, and trust knowledge in security applications have a positive impact on adoption but create a relationship between threat and intention. The findings do not provide a proper theoretical foundation but in the future days; developers may push the software diffusion over promising energy resources. Different case studies are taken out as a data collection process to analyze SaaS (Software as a Service) adoption by an organizational readiness. Users in the adoption of this technology process are involved with an intentional framework for key decisions that adopt the product [46].

Huda [47] explained the technology adoption with an empowering application strategy of ethical and professional engagement. Due to information technology, the world has changed dynamically and enabled people to engage with advanced concepts day by day. Administrative provision is essential for the positive implementation of technology. This work provides a reference model that empowers both ethical and professional application strategies with R and D in the adoption of new technology. This contribution improves the capacities and abilities

significantly for the utilization of organizational resources. Emerging technologies having personal and social awareness may impact the distinct facilities in an organization.

Smith and Ulu [48] emphasized the technology adoption process with uncertain future quality and cost in the decision-making process. A model is formed that explains uncertainty with the Markov process for the decision of technology adoption. First, it is required to do a simple NPV (net present value) analysis that compares the adoption, consideration, and possibility of technology in an organization. Secondly, through a stochastic dynamic program one-time event is formed that weights and views the possibility of technology adoption. The last model does not reject the repeated process and upgrades the new technology that suits more in the end. Due to the structural repeat-purchase design model, customized changes are performed that make technology improvement easy with better solutions.

Cost issues in the adoption of technology are considered endogenous variables that impact innovation performance. Due to cost issues, the performance of an organization is affected negatively as competitors adopt new technologies within shorter periods and special enhancements. The main aim of this article is to analyze the financial issues on technology innovation in various countries, especially for the Arab Spring. The variation in the source of funding impacts financial constraints due to different regulations and legislation. The designed model is a recursive bi-variate correctness to analyze the financial constraints that negatively affect technology adoption. Financial barriers and communication gaps among management become a big consideration these days in the adoption of technology and are seen with inclusion and negative impact [49].

Innovation adoption theory is used to explore different organizational factors related to adoption and users' decisions for an acceptance of new technology. The results conclude that top management support (internal) and competitive pressure (external) are critical factors in the direction of cloud technology adoption. A systematic review is prepared in this work for an organizational factor that impacts cloud-based technology adoption for an environmental framework. Cloud

computing technology brings big data analytics, and file storage that is secure and cost-effective with sustainable and flexible services for users [50].

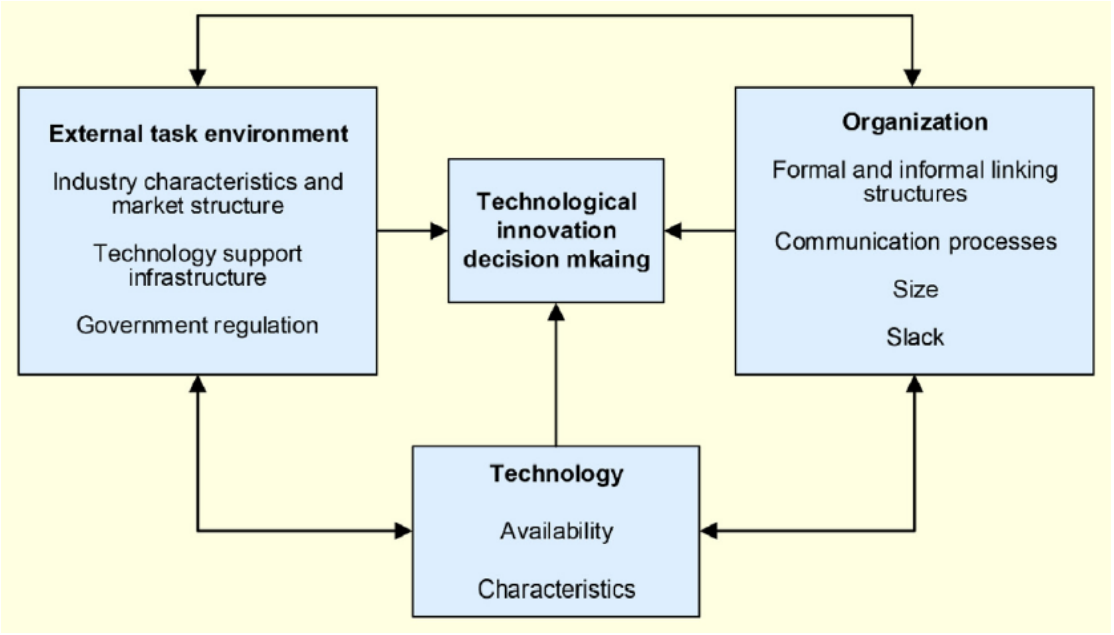


FIGURE 2.12: Organizational Factors in Cloud-Based Technology

Through data analysis of different organizations, it is identified that administration innovativeness is affected by power outages, capital budget, technology awareness corruption, R and D activities, foreign markets, provision training, and political instability. This study implies that employee training, quality labor, security policies, and foreign market covariates enhance innovativeness in technology adoption. This study investigated different aspects of political instability as well as sleaze in the adoption of new technology. The administration faced different problems related to political instability, and corruption in COVID-19 days [51].

New technologies are beneficial for an organization's productivity, easiness of management, valid communication, and cost efficiency. The innovation diffusion theory is reviewed and identifies the variables that impact innovativeness concerned with the administration of an organization. Technology innovation and adoption progress are slow in the agriculture sector as compared to the industrial sector due to competition and profit margin. The administration factors are explained in terms of technology adoption on agricultural productivity and global development. Agriculture sector technologies and drivers in technology adoption processes are not evaluated in detail. Some critical factors related to the administration are

analyzed such as the information transfer method, technology characteristics, economic influences, and socio-demographics [52].

The administrative intensity and organizational size have a stronger effect on the adoption of new technology as different stages are involved in it. Jeena and Philipson [53] clarified cost-effectiveness analysis, especially in healthcare sectors for technology adoption. Cost-effectiveness analysis is considered to be the best tool for increasing spending on new technologies in different sectors. The duties and liabilities related to new technology are defined by the management. This analysis process reflects prices that are set out optimally by different organizations other than their production cost and policies. Resource-cost treatments are important in every organization, as observations are taken through them, and paradoxical cost elevations can be avoided. Realistic theories are explained and after that differentiation between technology adoption and innovations is elucidated suitably.

Management factors are related to administration and influenced by human resource management and supply process procedures for recognition of the present market. Human management is concluded as the least relevant variable and declares clear responsibilities after adoption because technology investment reduces labor and production costs and significantly increases production quality. The adoption of adequate technologies with complete security policies is assessed for high performance in different types of organizations. Organizational culture must be developed to encourage and motivate employees for new technologies adoption. The main focus is to analyze technology adoption and its relationships among management and production-related traits [54].

In the research work of Moradi and Nia [55], a framework of TOE (technology organization environment) is analyzed with practical usage at feature and application levels in audit performance. The findings show that managerial support, employees' training, organizational size, and functional uses have a significant and positive impact on technology adoption and audit performance. All of the factors that affect the use of audit analysis are explained with a descriptive correlation study. Through technology adoption in auditing, the internal performance of an organization is improved significantly.

Seth et al., [56] evaluated the technology adoption in the health sector through administration factors that are marginalized. This work focused on users of HAMT (hospital administration management technology) through theoretical tests with an amalgamation of TAM and TPB to demonstrate significant factors and their impact on outlined elements. Through the data collection process of HAMT, it is identified that most health workers adopt technology due to PEU, PU, attitude, and subjective norms. The management could encourage employees and develop a culture of security consciousness to adopt new technology. Technology adoption is easy when users feel satisfied with their usage and find it useful in different aspects. It is suggested that time maximization and technology adoption enhance contextual factors of administration.

Nnaji et al., [57] elaborated on the technology adoption in the decision-making process with safety application and development for the construction field. Using new technologies in the construction field improves safety performance and effectively achieves the desired outcome. Administrative support and obligation are essential for the positive applied processes of new technology. The improved technology adoption leads to enhanced safety and reduces hazard levels on site. Multi-criteria decision-making (MCDM), TPB, and TAM models are evaluated and an adoption index is designed. This index identifies, quantifies, and categorizes user-friendly technology adoption factors.

Administrative factors are essential for technology adoption as managerial responsibilities, skills, and security rules knowledge are involved in its decision-making. The complexity of uneven internal structures builds major constraints in technology adoption related to an administration. Considerable cost reduction is very significant for the administration factor in the technology adoption process. Julien and Raymon [58] explained different factors related to technology adoption in retail sectors for small and medium-sized businesses. This work identifies different factors related to organizational, strategic, and structural means of software technology. The determinant factors identified include strategic pro-activeness, decentralization, time frame, clear responsibilities, affiliation, independent apprehensions, and availability of resources.

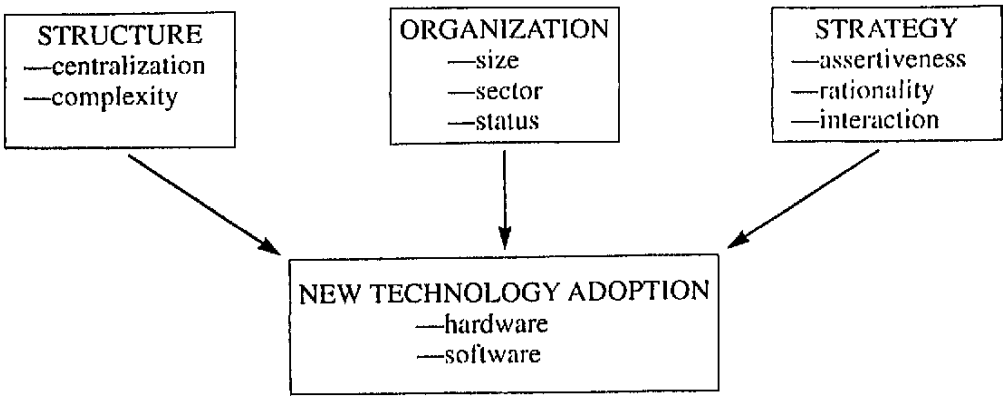


FIGURE 2.13: Framework of New Technology Adoption in Retail Sector

2.5 Theories of Technology Adoption and their Integration

2.5.1 Technology Acceptance Model (TAM)

TAM is known to be an information system that analyzes the way for the acceptance and usage of technology by users. This is the point in the actual system where the user uses the technology and behavioral intention leads towards the attitude and impression of the technology. The PEU and PU are the two factors presented in this model for the use of the technology.

Rad et al., [59] attempted to relate childhood education with postmodern concepts of TAM to assess how people adopt and practice new technology. New technology in the start goes with uncertainty so, in this work different scales are used to measure the PEU or PU. Intention to use new technology and a positive attitude of users are considered as main determinants for the usage of technology and improvement of security and safety in the future days. User training programs are arranged to help the successful adoption of new technology and compatibility among employees. TAM encompasses three elements such as environmental usefulness, economic usefulness, and social usefulness related to the technology. The model emphasizes different variables from the perspective of users and behavioral intention.

Acceptance and rejection of new technology are linked with human behavior. Due to incomplete information, uncertainty arises naturally during assessment. Perceived usefulness refers to the people who perceive and use the technology with observance to enhance or change their quality of life/tasks. Technology training programs facilitate successful adoption with fewer chances of rejection. TAM evolved with PU and PEU components to clarify the impact on attitude and behavior in technology adoption [60].

Alsharida et al.,[61] examined the empirical study of TAM for the past four years in the adoption of mobile learning. It is analyzed from the results that self-efficacy is a significant factor that disturbs mobile learning adoption and it is monitored by social influence, satisfaction, subjective norm, anxiety, innovativeness, and facilitating conditions. The organization considers the feedback and recommendations from customers after the adoption of new technology. For every innovation, advancements turn the predominant technology variable into different useful ways.

Behavioral intention is taken as the dependent variable along with a person's habit and the independent variable in system quality is considered for PEU and PU. PEU and PU are direct predictors of intention and quality influence usage for new technology adoption. After adopting new technology, safety and security must be enhanced from an organization's assets. TAM is extended in the research work for the acceptance of library applications. A limited exertion captures the positive and negative factors to encourage and engage customers for new technology adoption [62].

Investments and government policies for new technology adoption are linked especially with trust issues and insecurities that occur in the future days. The technology acceptance model is used to understand the e-learning technology usage by students on COVID-19 days all over the world. This research is conducted on the students as they are considered as the most active part of the society. The model is formed that is integrated with different factors from the user's perspective and provides awareness related to trust with an assessment scale. The sub-construct of TAM further discriminates against the second order which has social, environmental, and economic usefulness [63].

Berakon et al., [64] focused on the halal tourism sector with an expansion of TAM that mediates the relationship between PEU and PU. Some factors are found positively linked and determine the intention of an individual consumer towards halal tourism application technology adoption. Adopting new technology enhances the safety and security of an organization's equipment and assets. Different countries are taken as an example, where new technology frameworks are decentralized for private as well as national organizations. This work presented novel steps in the research framework and developed users' trust and knowledge of technology acceptance.

Technical attributes are derived from theoretical terms that enhance the explanatory power of adoption for practical implications. The usage of new technology depends on user behavior that is affected in different ways. More efforts toward the use of technology hurt users' attitudes but facilitate the resources with a positive trust to analyze the effect of technology acceptance. By probing of new technology acceptance, an explanation is provided under social context. Determinants are analyzed with intelligent information technology acceptance through digital transformation and sustainability. It provides a clue for information technology usage with improved sustainability and compatibility with user-friendly descriptions [65].

To handle both internal and external adoption factors of technology, recommendations are needed to gain technical awareness and programs for informational aspects. It is important to get feedback and recommendations from employees for an easiness of technology usage. Different factors are demonstrated for technology acceptance theories with a focus on artificial intelligence. Various acceptance theories are used for an explanation of AI-based products and consumer acceptance towards purchase. AI-based products increase the safety and security of an organization's assets after its adoption. Through decomposition analysis, different factors are included in the model but it is concluded that value-based adoption is considered the best for user acceptance [66].

Doubts and fears of adopting any technology are known as uncertainties and the person's expectations are dependent on PEU. Students from five universities in

UAE are undertaken to examine the acceptance of E-learning technology. Through past literature, external factors are identified as quality of the system, information content, self-efficacy, compatibility, and accessibility that have a significant impact on PEU and PU. The scales promote the individuals who answer the questions related to the context of complete research work. The responses obtained from the prompts can be used for internal assessment and responses about the framework [67].

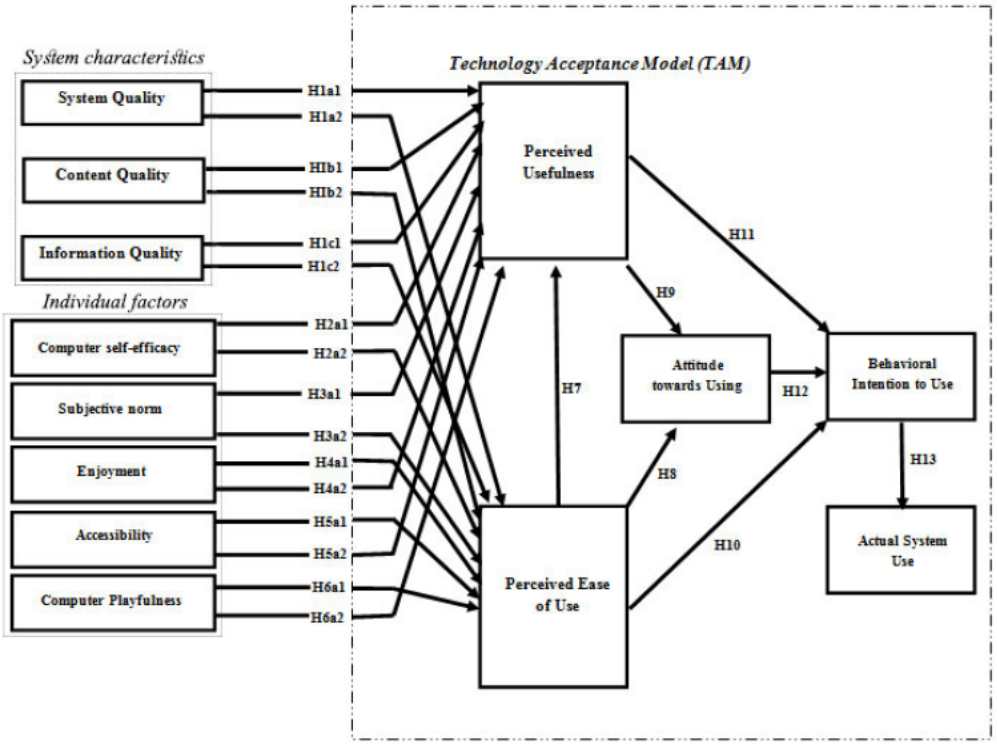


FIGURE 2.14: E-Learning Technology Adoption Factors Model

PU refers to the level at which users believe that using new technologies is easy with different means. Environmental usefulness ensures high-quality surroundings for future generations as it is essential to manage technology properly within the borderline. While utilizing technology, three aspects are considered such as perceived ease, attitude, and perceived usefulness. It is highlighted that consumer sentiments are fundamental to whether to accept or reject the technology. The user's motivation for an adoption is based on external stimuli like technology capabilities and features. TAM model gains insights into how different users accept the technology and after that adopt it suitably [68].

2.6 Supporting Theories

TAM is used as a foundation in terms of user behavior for acceptance of new technology. As this study is focused on the adoption of cyber-security locks; therefore, the user response to technology adoption and its influence can be explained with the help of the technology acceptance model. TAM was developed by Davis in 1989 as an information system theory that depicts how users of the technology can agree and use/take technology [60]. When new technology is offered to users, their choice is subject to two factors; (i) perceived usefulness (PU) and (ii) perceived ease of use (PEU). PU means how the user deliberates and supports the technology to improve performance. PEU is linked to how much the user employs the new technology. PU and PEU are observed as the central factors that promptly influence and elucidate the results. So, in this study, cyber security locks are introduced as a new technology from different organization's perspectives.

Cyber-security locks technology adoption in any organization can be clarified through this model. This theory turns out best with this research due to acceptance means in different terms and conditions. Whenever a new technology is introduced, the technology acceptance model is a suitable approach to observe the progress. There is a simplification function between intent to use and usage to overwhelm the barriers. Facilitation functions contain support, knowledge, training, and other belongings that help to use the technology more efficiently. The training and knowledge will be used as a facilitation function. Practically, perceived benefits related to the organization's response, proper communication, and professional meetings with higher authorities are necessary in this regard.

This research work mainly emphasized on adoption of cyber security locks and evaluated their acceptability in society and security-sensitive organizations. Roger's point of view for technology acceptance is an attitude/behavior whether they reject it or accept it. Adoption of new technology starts with the user learning related to the existence of an invention and understanding of working concerns. Choosing a new technology and innovation is not a quick action for any person, different steps are involved in acceptance. To make the acceptance model; there are five phases undertaken such as knowledge, persuasion, choice, application and

last one is validation/testing stages. Researchers have been using different theories for predicting the choice of the consumer for new technology but TAM is considered as the main theory in analyzing this research process.

2.6.1 Rogers's Theory of Innovation

Innovation diffusion theory is explained for management concerns through different communication channels and suggestions. The analysis is performed on the adoption and diffusion of mobile phones in India that become the key element in modern technology. Through communication channels, the prior conditions are set in practice with knowledge, persuasion, discussion, implementation, and confirmation. This study modified the existing theory, which is understandable for the consumer market, and attempted to work with constructional means around the world.

The product purchase intention among customers can increase profit because customers are mostly influenced by past beliefs and values. The product attributes are analyzed according to the consumers' intention and diffuse with a relative advantage such as observability, compatibility, trialability, and complexity. It is inferred that compatibility and trialability derive the decision toward the product purchase [69].

Khan et al., [70] explained the acceptance of sustainability innovation and environmental opinion by the diffusion of innovation theory. A survey is conducted that evaluates the adoption of sustainability in hospitals of Pakistan with data analysis through partial least SEM. The analysis shows simplicity, trialability, compatibility, and innovativeness role as it is important in the adoption of sustainable innovation.

A detailed discussion is reported on Roger's diffusion of innovation theory to find the community reactions to social innovation. It depends upon the emotional behavioral influence model to analyze how communities respond to the adoption of social innovations for development purposes. The community responses model is

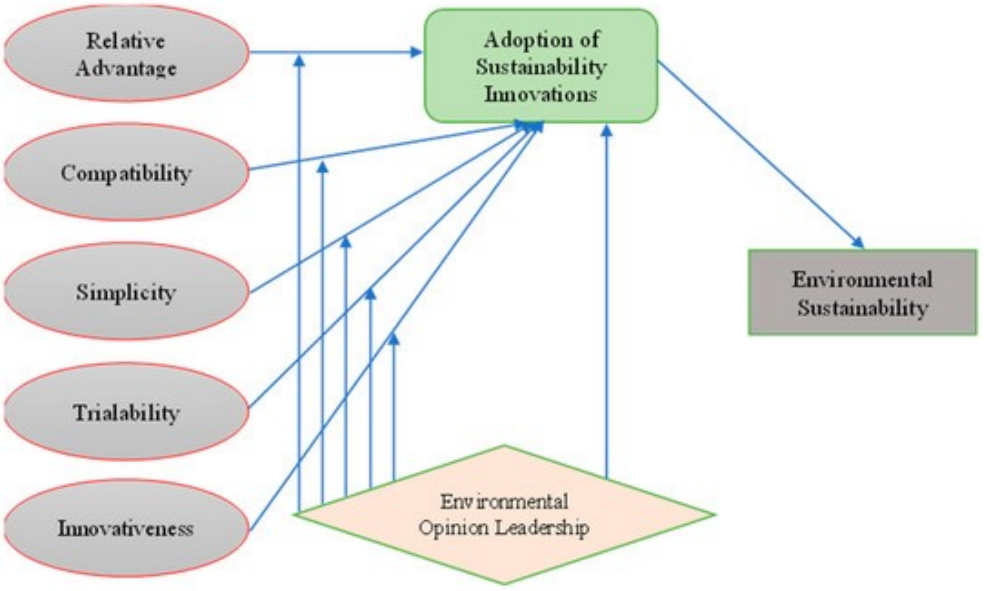


FIGURE 2.15: Sustainability Innovation and Environmental Opinion by Innovation Theory

divided into two groups; urban and rural worldwide to expand the overall significance of the study. As described in this research behavioral and social impacts on the communities are analyzed through innovations and motivational aspects [71].

Outcault et al., [72] analyzed unique features of distributed energy resources by adopting Roger's theory in technology characteristics. The tool for an assessment was developed for technology evaluation in which facilitation and adaptability address the characteristics of each distributed energy resource (DER). This work is structured from academic and industrial characteristics for the technology adoption process. Fourteen different technology characteristics are analyzed, which are yielded with coding, operability, and investigation.

2.6.2 Theory of Planned Behavior (TPB)

This theory is known as the cognitive social theory, which attempts to predict and explain human behavior properly. TPB covers constructs of behavioral control and subjective norms that significantly influence consumers. The research work conducted by Aboelmaged [73] elucidates the TPB with the integration of E-waste recycling. The model is designed to predict behavior that appropriately determines

the intention of e-waste recycling. About 47 percent of young consumers reflect good robustness and explanatory power towards this concept of e-waste recycling.

The TPB model is evaluated for three variables such as individual behavior variables, social behavior, and psychological variables. Individual behavior variables include smoking, exercise, eating, and many others in this list. Social behavior includes the person's interaction with other people and organizations for positive outcomes. Psychological variables attempt to predict and explain similar behaviors and social variables such as objects, events, culture, and societal values in which a person behaves with positive and negative aspects. The TPB extension is explained properly, in which the role of entrepreneurial intentions and motivations are discussed along with their application [74].

Subjective norms are considered positive and significant with an intention of using renewable energy resources. Attitudes toward renewable energy had no significant effect on usage; whereas, environmental concerns are considered as main intention toward renewable energy resources. The attention and different factors are analyzed for the usage of renewable energy with the TPB approach. The main determinants of attention are separated and the regression analysis is performed on the responses of the participants [75].

Individual attention and behavior are determined through attitude and subjective norms connected with perceived behavioral control. Individual attitude is an evaluation of the behavior that might be positive or negative prolonged at a high level. The TPB investigates different factors that predict the intentions with sustainability and challenging decisions. Green consumers identify attitudes, subjective norms, and perceived behavioral control towards sustainability with variance in intentions. The moderating role of green consumers is studied while engaging with their behaviors and intentions [76].

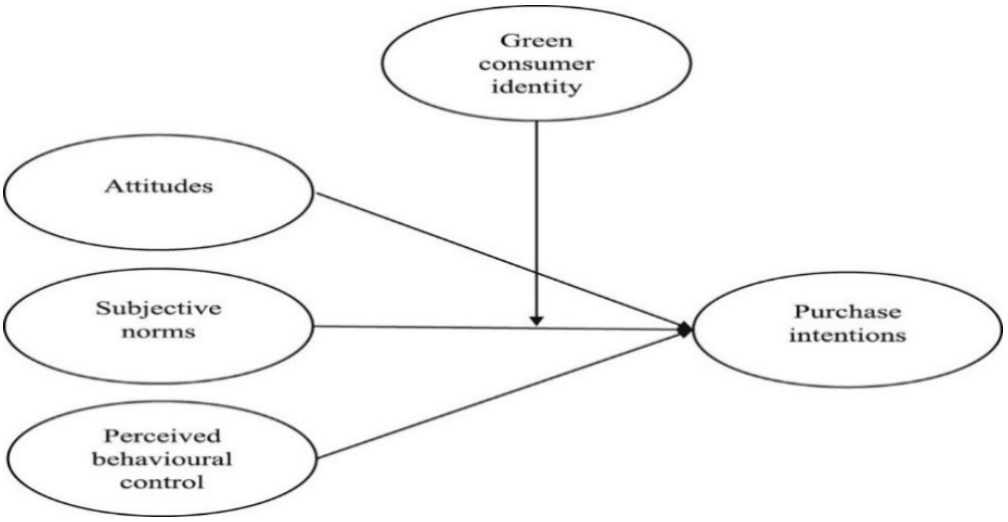


FIGURE 2.16: Model of Green Consumer and TPB

2.6.3 Technologies Integration

Perception of self-efficacy is undertaken as a certain action that may require complete skills, chances, and resources in the adoption of new technologies. The urbanization tendency has increased progressively due to the government and developed distinctive characteristics in terms of economics, resources, and energy growing concepts. Three theories TAM, TPB, and UTAM (Unified Technology Acceptance Model) are compared to assess fully automated vehicles (FAVs). There are external variables identified in this research study such as self-efficacy, perceived risks, and openness to technology to explore the perceptions of consumers related to cost and societal norms [77].

Cheng [78] conducted a comparison of the TPB and TAM theories to their predictive power and presented arguments in a precise context. The intention towards behavior and use of Wiki in group work by university students are evaluated in this research work. The partial least square SEM is used to measure more robust errors than regression-based SEM. After the analysis of the results, it is viewed that TPB is mediocre to TAM according to the concluded test values and evaluation processes in all variables. This work is threefold and reported that social influences have a vital role in collaborative e-learning processes.

The TAM is influenced positively by users and intensity to use the system, which is dependent on behavioral control, subjective norms, and attitudes. After emerging

both models of TAM and TPB, actual behavior and intensity seem to have a great impact on the utilization of the system. The apparent gamble hypothesis is drawn with features such as execution, security, monetary, social, and time risk. All of them are linked with an apparent coordination that is linked with TAM to utilize the goals of clients. This work investigates different factors that affect the behavior and intensity of users in an information system for state universities through TAM and TPB theories [79].

Hua and Wang [80] assessed the TAM and TPB models to analyze the intention toward energy-efficient appliances in China. Both models are used to identify perceived, social, attitudinal, and control factors that affect the acceptance of new technology. It is concluded that PEU has a vital influence on PU because consumer intention toward new technology is linked significantly with perceived behavioral control and subjective norms. This research examined the past acceptance of technologies by consumers and their behavior by combining both models (TAM and TPB).

The theory of innovation reference is important to understand in the method of blockchain technology and supply chain management. The inter-organizational trust and data transparency factors are studied. The results specify a noteworthy positive link between the value barrier, risk barrier, as well as image barrier for the practice of blockchain technology. The main goal is to meet technological, organizational, and environmental perspectives in blockchain technology adoption. It is required to enhance the system for leveraging security and managing the adoption factors that lead to non-technical countermeasures in a holistic way [81].

Different factors related to mobile banking are evaluated for the acceptance of advanced technology. The potential factors highlighted in technology adoption are economic, institutional, technological, and human-specific. These factors are investigated regarding blockchain adoption perception for banking customers toward new technology. The model in this research work is integrated with a unified theory of acceptance and use of technology, which shows that the combination of technical and managerial expertise makes the new technology adoption successful in any organization [82].

2.7 Research Gap

The smart lock-related studies are numerous with dominant adoption, innovative practices, and execution for past years, especially in developed countries. Researchers highlight the design and implementation of cyber-locks to a large extent but, adoption variables and their relationships are shaded and not addressed by researchers properly. An organizational-consumer behaviors measurement towards the cyber-security locks adoption is not measured easily due to external/internal perceived barriers and persistent needs. One and two variables combination are explained in different research but not explained individual sub-variables listed in previous research.

However, there is still room space available to analyze cyber-lock technology adoption barriers with the help of different technology adoption variables study. In adoption factors analysis, large efforts are presented by researchers, therefore the main aim of this research is to conclude the variables of new technology adoption. It is concluded that administrative variables, technical variables, TAM, and firm size play a very important role in new technology adoption.

To understand different technology adoption variables in an organization, seventy-eight (78) past papers are studied properly for literature knowledge. All researchers present their work related to these variables in revolutionary ways and demonstrate factors relations in a novel manner. Three main technology adoption variables with different relations among them are concluded i.e., technical factors (independent variable), administrative factors (dependent variable), firm size (mediator), and Technology acceptance model (moderator) in this work.

2.8 Summary of Literature

New technology adoption is improving day by day due to its central role in every field and organization. The success of an organization depends upon the advanced technologies and techniques used for its management. Cyber-lock technology is considered popular in different organizations but adoption barriers occur due to

different influencing variables. The covered literature summarizes the technology adoption variables and sub-variables that are linked in different ways. Technical variables and administrative variables are considered as main variables in technology adoption along with different sub-variables. Firm size is also considered essential in the adoption of technology and usually plays a moderating role between technical and administrative variables. The technology adoption model and TPB are considered in our work as important models for an analysis of new technology with their perceived usefulness. Privacy and security are considered as the main sub-factor in the acceptance of new technology accompanied by the cost at a high level. Cyber-lock technology gained popularity as a popular technology for managing security and privacy as it is a valuable tool in many organizations. Researchers have developed different models and analyzed variables that become barriers to the acceptance of advanced technologies. The combination of different variables model improves the thinking level related to adoption and improves the initial stages of technology adoption in an organization. Although, the existing literature reported the four types of variables and their contribution to technology adoption with different sub-variables; however, their combined effect has not been explored yet. As the adoption of new technology is not an easy task in any organization; therefore, the pros and cons of different variables related to new technology adoption are analyzed, which can be critical for successful adoption.

In the following chapter, the methodology will be elucidated in a detailed manner. The research model is designed after it combines the concluded technology adoption variables and relationships among each other individually. Three concluded variables are explicated with detailed discussion individually and the resultant hypothesis is also enlightened in detail.

After reviewing the literature on technical variables, administrative variables, and firm size; detailed sub-variables are identified that have been summarized in Table 2.1.

Table 2.1: Summary of Technology Adoption Factors Reported in Literature

Variables	Sub-variables	References
Firm Size	Revenues	[19][22][23][26]
	Resources and Assets	[21][26]
	Market Shares	[18][24]
	Capital labor ratio	[27][29][30]
	Market Changes	[23][24]
	Productivity	[19] [27][28][30]
	Number of Employees	[20][25] [26]
Technical Factors	Privacy and Security	[31][32][33][35][36][41] [45]
	Resource availability	[37][39]
	Operability/ Ease of Integration	[36][38]
	Technical Training	[34]
	Reliability and Efficiency	[35][41]
	Level of Complexity	[38] [49]
	Technical cost	[36][35] [41]
	Potential Risks	[40][43]
Administrative Factors	Top-level management	[46][50][52][53]
	Communication	[46][49]
	R and D (Research and Development)	[47]
	Security Policies and Procedures	[55][56][57]
	Cost (Budget)	[48][49][54]
	Allocation of Adequate Resources	[46][48]
	Security-Related Benefits Analysis	[43][51][53]
	Culture of Security Consciousness	[52][58]

Chapter 3

Research Methodology

In the previous chapter of the literature, a comprehensive literature is covered and the research framework is designed. This chapter explains the conceptual framework, thesis flow chart, research hypothesis explanation, research design, pilot testing, and data analysis. Data collection and statistical techniques are employed to ensure well-informed and rigorous research approaches. Technical Factors (TF) and Administrative Factors (AF) are related through Firm Size (FS) as a mediator and Technology Acceptance Model (TAM) as a moderator in cyber-security locks technology adoption analysis.

3.1 Research Flow Chart

In this thesis work; first, the technology adoption factors are identified through the comprehensive literature review. Four factors (FS, AF, TF, and TAM) are shortlisted after thoroughly revising the literature. The questionnaire is designed based on these four factors and then responses are collected from various security-intensive organizations. Testing techniques are applied to analyze the data and hypotheses. Finally, the conclusions are drawn based on testing results and analysis.

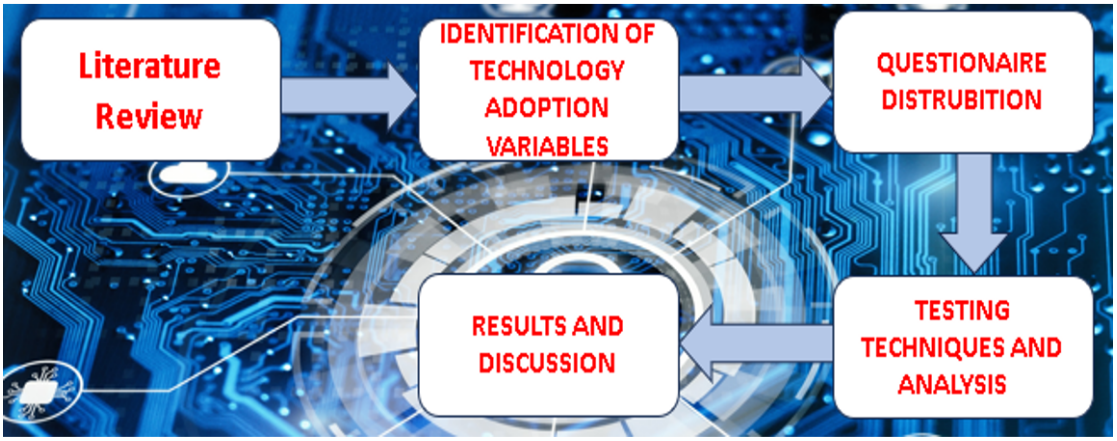


FIGURE 3.1: Research Flow Chart

3.2 Conceptual Framework

The goal of this study is to link adoption factors and organization-consumer behavior regarding cyber-lock technology adoption, particularly in Pakistan. As it is illustrated in the literature review, different theories are linked with technology adoption and implemented for organization-consumer behavior prediction.

Figure 3.2 describes the research model for the current study. Technical factors are independent variables that include different sub-factors concluded from the literature and affect the adoption of cyber-lock technology adoption. Firm size is employed as the mediator between dependent and independent variables. Administrative factors are designated as dependent variables in cyber-lock technology adoption, which means that they may be affected by the mediating variable (firm size). The TAM acts as a moderator between technical and administrative factors (TF and AF) with the user perspective control. It means that any change in moderator will influence the relationship between TF and AF. In order words, if a moderator (TAM) increases in an environment, the technical factors are determined based on this increment and then administrative factors are augmented accordingly.

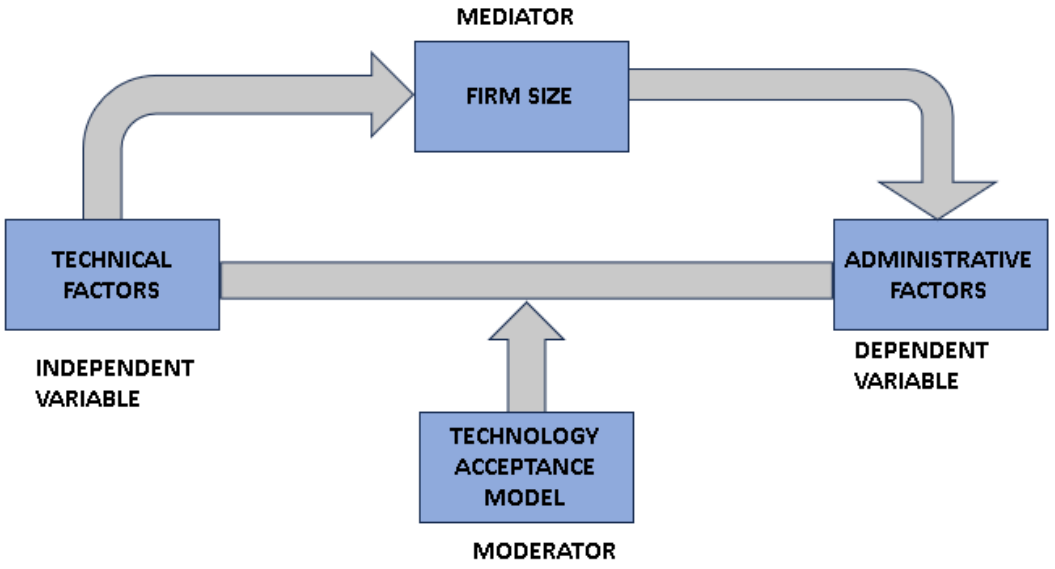


FIGURE 3.2: Research Model

3.3 Development of Research Hypothesis

This study assesses the willingness of an organization to adopt the cyber-lock technology. As a result, hypotheses are designed along with the main components formulated from the research model. Three hypotheses are inferred based on different findings from the literature work related to the organizational-consumers factors.

H1: Technical factors (TF) have a positive and significant relationship with administrative factors (AF).

H2: Firm size (FS) mediates the relationship between technical and administrative factors (TF and AF).

H3: Technology acceptance model (TAM) moderates the relationship among technical and administrative factors (TF and AF).

3.3.1 Technical Factors

The technical factors in the adoption of new technology play an important role as they belong to sensitive details and technological means. The physical experience and qualities belong to the parameters that lead to the level of involvement in

an organization. Technical factors affect the variables that have an existence, development, and availability for the technology. If technical factors are satisfied then the adoption of cyber-locks is possible in an organization under different terms and conditions related to the security means.

The sub-factors of the technical category that are involved in the adoption of cyber-lock technology are:

- Privacy and Security
- Resource Availability
- Operability/ Ease of Integration
- Reliability and Efficiency
- Level of Complexity
- Technical Cost
- Potential Risks

The results show that the technical factors are independent of the adoption of cyber-lock technology in an organization. Improvement and strong settlements are required for technical factors, which is possible when organizational factors are implemented through advanced means. Firm size factors mediate between organizational administrative factors and the technical factors; therefore, organization sales, revenues, and others are taken into account from the technical factors advancements. As a result, from the literature, it is concluded that the technical factors are critical in the adoption of cyber-lock technology, and these are also important to control administrative factors and barriers for effective solutions.TAM is moderating between technical and administrative factors as user attitudes and perspectives impact technology adoption. Perceived usefulness and perceived ease of use collectively control the user's behavior factors included in the technical and administrative factors list. The independent variable causes a change in the dependent variable; technical factors impact administrative factors by user's behavior. If technical factors are fulfilled then administrative factors are managed easily through the moderating effects of user's behavior.

3.3.2 Administrative Factors

Administration in any organization plays a very important role in managing functions through different procedures and factors. Both internal and external management of an organization's affairs are involved in this category for new technology adoption. There are different terms and conditions over which administrative factors occur in the adoption of new technology for an organization. Operative communication and coordination with administrative factors improve the technical factors as well due to direct relation with it and enhanced efficiency. Through an effective management system, operational concerns, leadership skills, transparency, trust building, benefit giving, and listening make the administration perfect. Technical factors are taken into account first in an adoption, and due to these administrative factors are considered as dependent ones with different terms and conditions. The subfactors of the administrative category concluded from literature work involved in the adoption of cyber-lock technology are listed below:

- Top-level management
- Communication
- R and D (Research and Development)
- Security Policies and Procedures
- Training Programs and Awareness Campaigns
- Cost (Budget)
- Allocation of Adequate Resources
- Security-Related Benefits Analysis
- Culture of Security Consciousness

The findings suggested that administrative factors are dependent on the adoption of cyber-lock technology in an organization. After improving administrative factors technology adoption becomes easy and the attention of employees increases toward new technologies. These factors are dependent as it only linked with organizations and consumers for external and internal means. Sometimes, it behaves as internal factors and sometimes as external depending upon different situations and countermeasures. If administrative factors are contented then, adoption is

plausibly related to the cyber-locks in an organization through firm size measurements and their subfactors. Technology acceptance is moderating among technical and administrative factors as user attitudes and perspectives impact new technology. Related to the given technical hypothesis (H1) and different backgrounds of an investigation, it was expected that administrative factors are dependent on technical factors in cyber-security locks technology adoption.

3.3.3 Firm Size

The firm size is analyzed through different studies as it employs different measurements such as sales, total assets, revenues, and market value equity, no of employees over an organization. In some organizations firm size also includes financial policy, dividend policy, investment, managerial compensation, diversification, firm performance, and linked corporate governance. The subfactors of firm size that are involved in the adoption of cyber-lock technology are listed below:

- Revenues
- Resources/Assets
- Market Shares
- Customer Demands
- Capital labor ratio
- Productivity
- Number of Employees

Based on different findings, it is explained that firm size is important in the adoption of technology and acts as a vital factor that directly affects it. It is recognized that organizational motivation and courage are increased with a positive effect on firm size otherwise less attention is shown by an organization. Administrative and technical factors are improved when firm size increases positively and becomes beneficial for an organization. In the case of cyber-lock technology adoption, the firm size is discovered as a mediator in positive means with different solutions. Different organizations calculate firm size in technology adoption at the initial stages but it varies from time to time due to administrative and technical factors. The

firm size is explained through different schemes and methodologies by numerous authors in their studies and is considered an important parameter for technology adoption processes.

3.3.4 Technology Acceptance Model

TAM postulates the acceptance of technology by the users (employees and consumers) and is determined by the usefulness of technology in task performance and PEU. Through TAM, user behavior is defined through a framework that gains technology insights in two ways; (i) by accepting the technology, and (ii) by adopting it properly for an organization. The utilization of technology is governed by two aspects; perceived ease and perceived usefulness. It is observed that the sentiments of the consumer are the fundamental concerns whether they accept or reject the technology. The two primary components related to TAM are depicted through the behavior of employees and the consumers of the technology. From the findings of different studies, it is analyzed that the TAM acts as a moderator to make a better understanding of user acceptance and answers how technology is impacted by an interaction of both technical and administrative variables. Due to the TAM involvement, successful implementation of technology is observed with an informed decision-making process. User's positive attitude towards new technology makes technology use easy and enhances collaboration and integration between both independent and dependent factors.

3.4 Measurement and Data Collection

An extensive literature is covered to identify and analyze measurable concerns for the current research work. In this regard, the firm size-related research work is used to measure adoption factors for technology adoption. The past work for administrative factors is used to identify sub-factors and develop links for cyber-lock technology. The research work of different researchers related to technical factors is used to determine sub-factors closely linked with cyber-lock security

features. Based on different findings of the literature review, a research factors-related questionnaire is developed to collect responses (provided in Appendix I).

3.4.1 Research Philosophy

This research is based on the past concepts reported in numerous research studies to support and explain the hypotheses and to verify them empirically. The quantitative method is used with different research techniques for data analysis. Measuring and quantifying variables are used that answer the research question and objectives with relationships among them. The conclusions are deduced from the hypotheses and compared with data test judgment of pass or fail criteria.

3.4.2 Unit Of Analysis

The unit of analysis determines individuals, organizations, and different geographical locations, that are related to the current research work. The participants included in the current research work are selected from the technical fields, who have good know-how and experience of the all factors used in the research model. Diversified organizations are included in responses such as banks, defense institutes, customer services organizations, cyber-security vendors, and all types of security-sensitive organizations. An online Google Form is used to gather responses through the questionnaire designed in the English language. This online data collection process is easy, convenient, and cost-effective as explained by Fischer et al.,[83].

3.4.3 Sample Size

The sample size taken for our research work is 400 which is an ideal size and reliable for our research framework and goals. This sample size is determined through the Rawalpindi and Islamabad city population size, our research objectives, and statistical considerations. In general, a large sample size represents more reliable results but it could require more resources and time. Our resources and desired level of accuracy meet this sample size so, this is selected with probability sampling

in which every individual has an equal chance to represent. To calculate the sample size of our work Taro Yamane formula is used in which N is the population under which the study is undertaken, and e is the margin error which is taken as 0.05 in our study [84]. The population of Rawalpindi city in Pakistan is 2,377,000 and Islamabad is 1,232,000 by combining both cities population is almost 3.6 million. All values are put in the formula for the research sample size calculation.

$$n = \frac{N}{1 + N(e)^2}$$

$$n = \frac{3609000}{1 + 3609000(0.05)^2}$$

$$n = 399.9\ approx 400(ideal\ sample\ size)$$

In general, a large sample size represents more reliable results but it could be expensive due to more utilization of time and resources. The selected sample size is reasonable to meet the desired level of accuracy as it is selected based on probability sampling and every individual has an equal chance to represent.

3.4.4 Population

To carry out the current research work, the security-sensitive organizations of Rawalpindi/Islamabad (Pakistan) region are selected. In the initial stage, 30 responses were taken for pilot testing, after that the remaining feedback was gathered, which contained 322 valid responses, and only these responses were considered for the current testing study. The population contains professionals with subordinates, stakeholders, managers, staff members, and team leaders related to this field. This model is applied to different organizations that are sensitive to security means. The data is collected through a Google form (questionnaire), which is filled and submitted by the respondents Wolverton [85]. The questionnaire is divided into two sections; the first section is related to personal information, and the second section covers the firm size, administrative factors, technical factors, and the TAM. The responses are disseminated and gathered online and then data is compiled for analyses from the selected population.

3.4.5 Sampling

It is quite challenging to manage and collect data from different sources due to some limitations related to resources, security issues, and time-related constraints [86]. The sampling technique used in our research work is the non-probability sampling technique type named purposive sampling. In this sampling technique, the population members are selected that are good prospects for accurate information. For our research work, professionals in cyber-security are selected that provide valuable information properly for our work. The sampling techniques used for the data collection distribute the individuals in the groups for a true representation of the whole data population. The respondents are required to fill out the two sections, in the first section, the respondents provide complete information that is considered personal information like demographics including age, gender, and experience. The second section is divided into four parts, which cover the questions related to the factors selected for the current study. Nemoto and Beglar [87] enlighten the Likert scale as an appropriate tool to measure the respondent's viewpoint about certain knowledge, opinion, behavior, and attitude. The Likert scale used in the current work is a five-point range to measure the responses with categories of strongly agree "1", agree "2", neutral "3", disagree "4", and strongly disagree "5".

Sample groups are divided into three main categories from which the data collection process is accomplished. The contributors to the research are professionals at the management level of various organizations. The first category includes different organizations that are currently using cyber-security lock technology in their organizations. The second category includes companies that act as vendors and provide different cyber-security services in Pakistan. The third category is related to security-sensitive organizations that include banks and some defense area professionals who are well-known in cyber-security technology. The demographic is statistics of the research that is related to the audience and maintains an important element of the research work [88]. The characteristics study includes gender, age, and experience of different levels of the targeted audience. Advanced technology awareness among professionals in organizations plays an essential role

in the success of any nation through which they compete globally. Maximum respondents in this research have knowledge related to cyber-security and work in project-based and/or operation-based organizations. An operation-based organization has experienced people, who may answer properly with clear concepts and explanations.

3.5 Testing Types and Data Analysis

Data analysis is the process that contains computational and statistical methods for the extraction of valuable information from the data [89]. The reliability of responses is tested through Cronbach's alpha technique. Data analyses require a combination of different skills that include technical, social, and interpretation of results. Complete data is analyzed through the AMOS (Analysis of Moment Structures) tool of SPSS (Statistical Package for Social Sciences) software along with hypothesis testing using SEM (Structural equation modeling) that evaluates the hypotheses of the study and model fitness. The results of this study permitted and focused on the exploration gap for grouping novel variables with reasonable structure investigation.

Different tests that are performed in the current research work are listed below:

i. Confirmatory factors analysis (CFA).
ii. Descriptive statistics.
iii. Regression analysis.
iv. Mediation analysis.
v. Moderation analysis.
vi. Correlation analysis.
vii. Reliability test.
viii. Hypothesis testing.

Chapter 4

Results and Discussion

The research methodology elaborated in Chapter 3 would be applied and tested on the research model of the study. All of the responses collected from the questionnaire are inserted in SPSS software for testing and the results are evaluated in various ways. Selective tests related to the current research are performed that are listed in the previous chapter. As a result of these tests, the hypotheses are assessed and decisions of acceptance and/or rejection are finalized.

The research model is examined through structural equation modeling (SEM) confirmatory factor analysis (CFA) by using the AMOS module of SPSS software for analyses. The SPSS is a suite of key software programs that analyzes research data with fast-visual modeling processes examined in a scientific way [90]. Through AMOS, the analysis of the research model becomes easy and understandable from different perspectives. SEM by using AMOS is a powerful tool for the analysis of complete structure as it is easy to use, specify, view, and modify according to model requirements [91]. Data is revealed through four main variables defined in SPSS: Variable 1; Firm Size, Variable 2; Technical Factor, Variable 3; Administrative Factors, and Variable 4; Technology acceptance model. All factors are interlinked with each other directly or indirectly with mediating, moderating, direct, and indirect relations. In the current work, CFA in AMOS is used to check model fitness and to conclude significant results. According to different testing processes,

concluded results determine whether the hypotheses are true or false and whether the research model is fit or not.

4.1 Results and Demographics

Demographics include the respondent's gender, age, and experience described further with a graphical representation of percentages.

4.1.1 Gender

Most organizations include two types of genders, male and female. In the figure 4.1 given below, male respondents are 71.98%, which is more than female respondents of 28.02%. Male respondents are high in our data collection process because in many organizations the ratio of male employees is larger as compared to females, especially in the industrial sector.

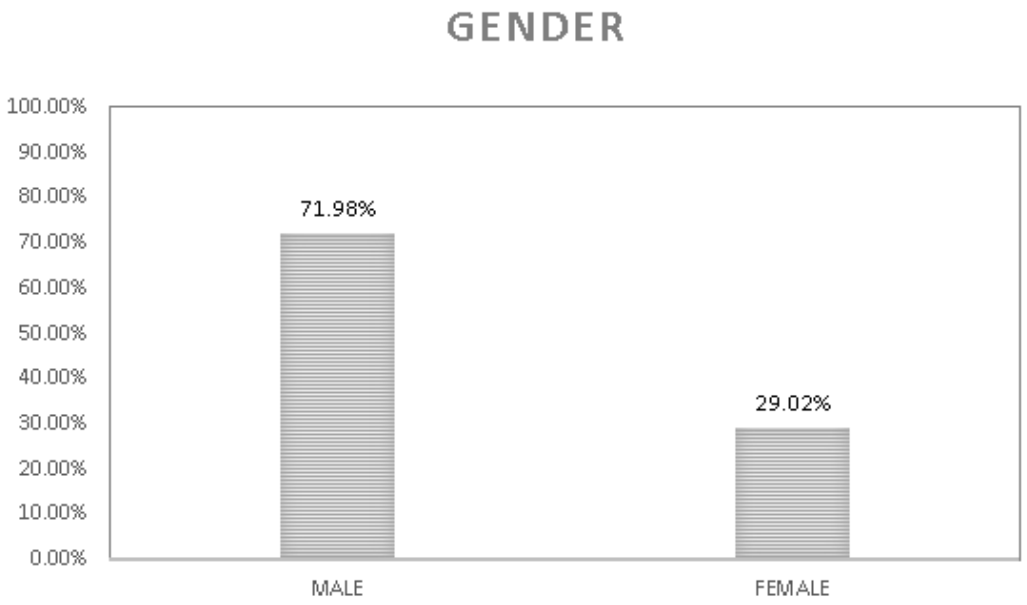


FIGURE 4.1: Gender category respondents

4.1.2 Age

People of different age groups of are included in the current study, so three choices are given to the respondents. In the choice of 20-30, the respondent's percentage is 18.45%, they are mostly interns and have less than five years of experience in an organization. In the age category of 31-40, the respondents are higher in percentage as they are professionals and known for advanced technologies, so they answered the questionnaire more precisely with 46.80%. An intermediate response is obtained from the above 40 age group as they have more experience but in the selected population, the percentage is 34.75%. All age responses are shown in the following figure 4.2.

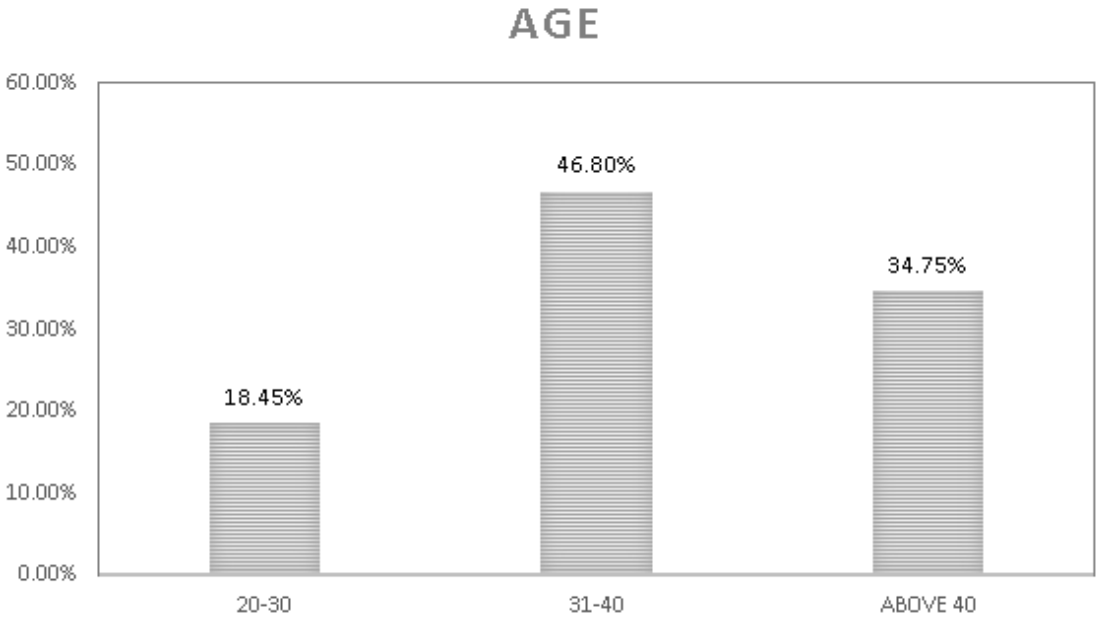


FIGURE 4.2: Age category respondents

4.1.3 Experience

In the figure 4.3, the respondents that have an experience between 1-5 years are 9.51%. The respondents with an experience of 6-10 years are 51.02% as they are youth and more familiar with advanced technology. The respondents above 10 years of experience are 39.47% and their information is more fruitful.

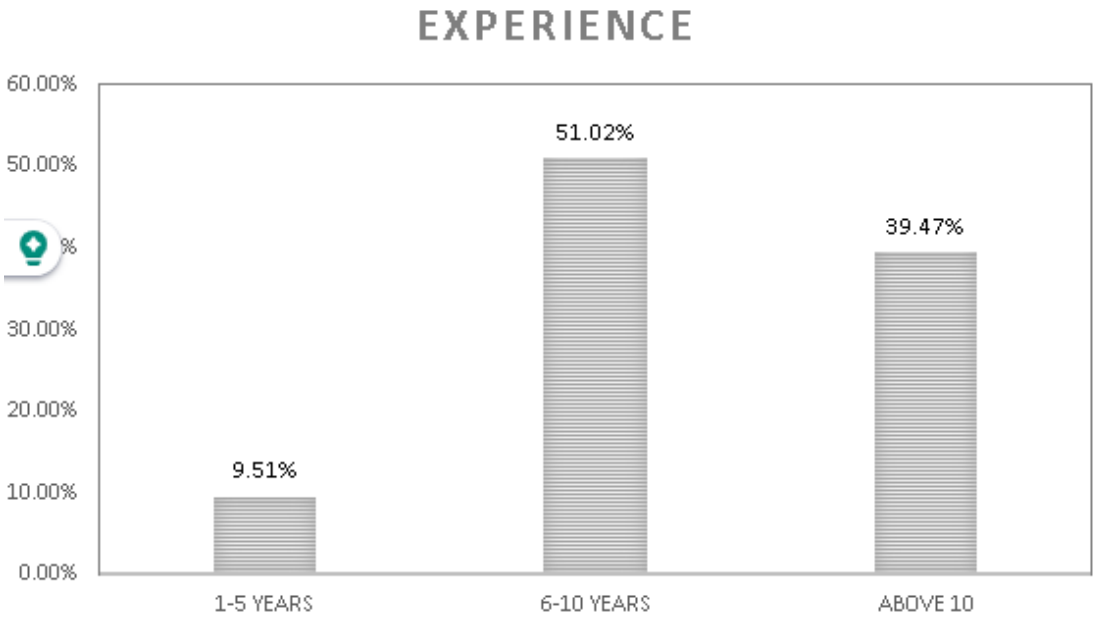


FIGURE 4.3: Experience category respondents

4.2 Structural Equation Modelling

Structural equation modeling is the linear model framework, which is used in this work to analyze the relationships among variables that are perceived to be complex and not understandable easily. In the current model, both direct and indirect relationships are examined that occur among variables, and underlying mechanisms are understood properly through SEM. Kline [92] explained different types of SEM, which are considered in research work according to the goals. The most common type is CFA, which validates the measurement properties related to the constructs. Path analysis is also the main type in which relationships among variables are analyzed in detail. Full SEM is used to analyze both direct and indirect relationships among variables. Regression, mediation, and moderation processes are also conducted within the framework of SME [93]. In our research work, all the analyses are performed to evaluate the research model and conclude through hypothesis testing by acceptance or rejection.

4.3 Pilot Testing

Different uncertainties appeared at the start of the questionnaire distribution phase, which is related to the question's reliability and validation. To deal with these uncertainties, pilot testing is performed that is applied to a minimum number of 30 responses as elucidated by Smith [94]. Through data validity, variable errors are analyzed and corrected in the questionnaire to ensure the reliability of the research study. At the start, more than 30 responses should be taken out to check the reliability test so in this research 40 are taken which is 10 percent of the sample size, and check whether the questionnaire is reliable or not. Values of Cronbach alpha are less than 0.7 in pilot testing so, two items one from AS and the second from TAM are deleted because these items' responses are fluctuating and disturbing. After deleting two items the reliability of AS increases from 0.62 to 0.71 and TAM from 0.67 to 0.74 which becomes an acceptable range.

4.4 Reliability Test

The reliability test in this research work is performed through internal consistency in two ways, composite reliability and Cronbach's alpha. The difference between both values is small, which represents a good reliability of the responses obtained through the questionnaire. Reliability is the degree to which the research method is consistent and stable. Both types of reliability analyses are performed to evaluate the consistency of the responses.

In the Cronbach's alpha reliability test, data is examined through SPSS software by analyzing and then selecting a scale with a reliability analysis type. After that, check the Cronbach's alpha value for each variable, which is included in the model[95]. For the analysis process, every variable and its concerned items are run in the software as they rely on the classical theory of assumption, and the value is improved by deleting the items. It is suggested that the minimum value must be 0.6 for an acceptable level of reliability [96]. To accomplish this; first, select the analyze tab and after that scale it and choose the reliability analysis. Cronbach's

alpha values indicated the internal consistency that is acceptable with a value of 0.6 and above not less than it [97].

TABLE 4.1: Cronbach's Alpha values

Variables	SPSS name	No. of items	Alpha values
Firm Size	**FS**	8	0.908
Administrative Factors	**AF**	9	0.894
Technical Factors	**TF**	7	0.902
Technology-acceptance model	**TAM**	5	0.814

All the results related to the analyses of variables and items are enlisted in the table 4.1 of the reliability test (Cronbach's alpha). The firm size has eight items and has a value of 0.908, which is the highest among all studied variables. Administrative factors obtained a value of 0.894 and a total nine items are included in this variable. Technical factors achieved a value of 0.902 and items in this variable are seven in number. The technology acceptance model contains five items and its Cronbach's alpha value is 0.814. From the results, it can be noted that Cronbach's alpha values of all variables are higher than 0.7, so it is concluded that all items are reliable and have an acceptable range of reliability.

Composite reliability is performed in Excel® through SPSS by the formula of composite reliability and average variance extracted to measure the consistency of variables loading over the latent variables [98]. It is used in exploratory factor analysis; whereas, Cronbach's alpha is used for confirmatory factors analysis in an advanced fashion. Composite reliability should be equal to or higher than 0.7 for good reliability results [99]. To calculate the value of "£" in the formula, the factor loading of variables is done that is known and identified through SPSS.

For the calculation of composite reliability, the above-given formula is used to compute the results. In SPSS analysis, the dimensions are reduced with factors and after that, all factors are checked with maximum variance computed in the table 4.2. The rotated component matrix is used to analyze factor loading and select only those values that do not occur in the merged way with other variables.

$$Composite\ reliability = \frac{(\sum £)^2}{(\sum £)^2 + \sum \mathrm{ME}}$$

£= factor loading

ME (measurement error) = $[1-(\sum £)^2]$

$$Average\ variance\ extracted\ (AVE) = \frac{(\sum £)^2}{N}$$

TABLE 4.2: Composite Reliability and Average Variance Extracted Values

Variable	Composite reliability	AVE
Firm size	0.81	0.53
Administrative-factors	0.84	0.67
Technical factors	0.80	0.54
Technology-acceptance model	0.78	0.51

The comparison of the two reliability tests presented in Table 4.3 exhibits that there is a very small difference between Cronbach's alpha and composite reliability. All variables in both reliability tests achieved higher values than 0.7, which means that the responses received against all constructs are significantly reliable.

TABLE 4.3: Comparison and Difference of Two Reliability Tests

Latent Variable	Cronbach-alpha	Composite Reliability	Difference
Firm size	0.908	0.88	0.028
Administrative-factors	0.894	0.87	0.024
Technical factors	0.902	0.89	0.012
Technology-acceptance-model	0.814	0.81	0.04

4.5 Pearson Correlation Analysis

Pearson correlation is used in this work to assess the relation among different variables in the model [100]. The direction and strength between two variables

are defined in this analysis as one variable changes, other one is also changed in the same manner. This method is known to be the very basic statistical process for analysis in statistics with frequent implementations. Pearson correlation is represented by "r" and its range should lie between -1 to 1 as the strength of two variables is compared with the degree of value of "r". Gogtay and Thatte [101] defined that in the range between +0.5 to +1, there is a positive correlation among variables, and in the range from -1 to -0.5, there is a negative correlation among variables. Values near zero show weak relationships among variables, so it's good if the value is far from zero. Considering these criteria for the current work, all variables show a positive correlation with each other as all values lie between 0 to +1 range.

Technical and administrative factors have a positive and significant relationship that has an R-value equal to 0.818** and a p-value less than 0.01. Firm size correlation with administrative factors has a value equal to 0.758** with a p-value less than 0.01. Firm size correlation with technical factors has a value equal to 0.792** with a p-value less than 0.01. The technology acceptance model moderates the relationship between technical and administrative factors and has a positive and significant relationship with a p-value less than 0.01. Technology acceptance model correlation with firm size factor has a value equal to 0.798** with a p-value less than 0.01. Technology acceptance model correlation with administrative factor has a value equal to 0.790** with a p-value less than 0.01. Technology acceptance model correlation with technical factor has a value equal to 0.811** with a p-value less than 0.01. The correlation results of all factors are shown in Table 4.4.

TABLE 4.4: Correlation Analysis

Factors	**FS**	**AF**	**TF**	**TAM**
FS	1			
AF	.758**	1		
TF	.792**	.818**	1	
TAM	.798**	.790**	.811**	1

4.6 Descriptive Statistics

All values like the total respondents, minimum value, maximum value, mean value, and standard deviation are given in Table 4.5. The letter N shows the number of respondents and the mean value (the average value). The highest value std. dev (0.9587) attained by the administrative factor (AF), and the lowest value (0.81602) belongs to the Firm size (FS).

TABLE 4.5: Descriptive Statistics Analysis

Factors	N	Minimum	Maximum	Mean	Std-Deviation
FS	322	1.00	5.00	2.3991	.81602
AF	322	1.00	5.00	2.2602	.95847
TF	322	1.00	5.00	2.5106	.83187
TAM	322	1.00	5.00	2.4360	.85055

4.7 Regression Analysis

Regression analysis is a statistical procedure that calculates the change in the dependent variable concerning the independent variable from observed data of the research [102]. An estimation of the relationship between dependent and independent variables is described with the strength of future concerns between both variables. Arkes [103] enlightened the main purpose of regression analysis as it identifies the causal relationship and defines how the treatment variable (independent variable) has affected the outcome variable (dependent variable). In the current research work, the Hayes A.F. technique is used for regression analysis with both mediation and moderation impact of independent and dependent variables [104]

From the regression analysis results, it is analyzed that the independent variable (technical factors) shows a significant relation and direct positive link with the dependent variable (administrative factors). An increase in technical factors will inevitably increase administrative factors when the value of p is less than 0.01,

which is 0.0000, and the beta is equivalent to 0.639 beta range lies between 0 to 1 or 0 to -1, reliant on the direction of the relationship which may be positive or negative). Hence, it can be concluded that there is a significant relationship between the independent variable TF and the dependent variable AF. Alternatively, any decrement in technical factors will cause a relevant decrease in administrative factors, as it has a positive impact. R square has a value of 0.407, which is the degree of variability; it means that our independent variables (TS) cause a change of 40% in the dependent variable (AF). Therefore, Hypothesis 1 "technical factors have a positive and significant impact on administrative factors" is accepted.

TABLE 4.6: Regression Analysis

Administrative factors			
Predictors	β	R^2	p
Technical-factors	0.639	0.407	0.0000

4.8 Mediation Analysis

Mediation analysis is used to analyze the relationship by discovering a mechanism in which one variable influences the second variable through the mediator variable. From the data, the relation of mediation is defined by full, partial, and no mediation among independent, dependent, and mediator variables [105]. The causal relationship "p" and its effect on process analysis facilitate the agreement by both parties and mutually applied decisions. Abu-Bader and Jones [106] explored the influences of the indirect effect of an independent variable on the dependent variable through the mediator variable. The mediator acts as a neutral variable that assists variables in negotiating different ways with positive output. The overall direct and indirect effects are analyzed with their consequences through comprehensive demonstration related to mediation analysis [107].

In the current research work, two methods are used to analyze the mediating variable effect on independent and dependent variables. One way is through SPSS software with the plug-in of Process by Andrew F. Hayes and model 4 is used for

the mediation process [108]. The second way is through the AMOS module of SPSS software to analyze the mediation effect and significance of variables.

4.8.1 Mediation Analysis through SPSS Software

This approach offers a chance to examine the mediation effect and prevent the flaws related to the different theories described. Administrative factors work as the dependent variable and technical factors as the independent variable to perform mediation analysis. The process macros of SPSS perform the results and utilize the outcomes reasonably. All values highlighted in Figure 4.4 with yellow color are important to be considered for the results of mediation analysis. It may be presumed that the firm size acts as the mediation variable described in Hypothesis 2. The mediation analysis is performed in SPSS and undertaken using the approach of bootstrapping. Through a 95% confidence interval, the method is established as related to the bootstrapping approach and has to work by an indirect effect with estimation. Through the selection of model 4, the mediation analysis is accomplished.

```
Model  : 4
    Y  : AF
    X  : TF
    M  : FS
Sample Size:  322
OUTCOME VARIABLE:
 FS
Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .7923      .6278      .2486   539.6895     1.0000   320.0000      .0000

OUTCOME VARIABLE:
 AF

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .8376      .7015      .2759   374.8358     2.0000   319.0000      .0000

****************** DIRECT AND INDIRECT EFFECTS OF X ON Y *****************

Direct effect of X on Y
     Effect         se          t          p       LLCI       ULCI
      .6718      .0578    11.6290      .0000      .5581      .7855

Indirect effect(s) of X on Y:
       Effect     BootSE   BootLLCI   BootULCI
FS      .2705      .0595      .1571      .3893
```

FIGURE 4.4: Mediation Analysis Results in SPSS

To quantify the indirect impact related to technical factors, administrative factors, and firm size, the lower limit (Boot LLCI) and upper-level intervals (Boot ULCI) are between +0.1571 and +0.3893, it simply meant that no zero (0 value) occurred in this range. Therefore, the firm size acts as a mediator between technical and administrative factors with significant relation. As the value of p-value is 0.0000 for firm size (which is less than 0.05); thus, it effectively mediates the administrative and technical factors. Both ULCI and LLCI are positive, if any value from both is negative then the firm size could not mediate between technical and administrative factors. Therefore, it can be claimed that the mediation takes place. Hence, Hypothesis 2 "firm size mediates the link between administrative and technical factors" is accepted. The mediation analysis results with direct and overall management including indirect effects and their consequences are shown in Table 4.7.

***LLCI: lower limit confidence interval

***UCLI: Upper limit confidence interval

***X: Independent variable

***Y: Dependent variable

TABLE 4.7: Mediation Results in SPSS

Direct-effect	**Indirect-effect**	**Total-effect**	**BootLLCI**	**BootULCI**
0.6718	0.2705	0.9423	0.1571	0.3893

4.8.2 Mediation Analysis through AMOS Module

The mediation analysis is also conducted by using the AMOS module of SPSS software, which allows the testing of the indirect relation of an independent variable on the dependent variable by the mediator (third variable). First, the effect of the independent variable (TF) on the dependent variable is checked without mediator involvement. The effect of the independent variable on the dependent is 0.65 as the direct relation between both variables. There is a significant relation between independent and dependent variables as represented by the P in 4.5.

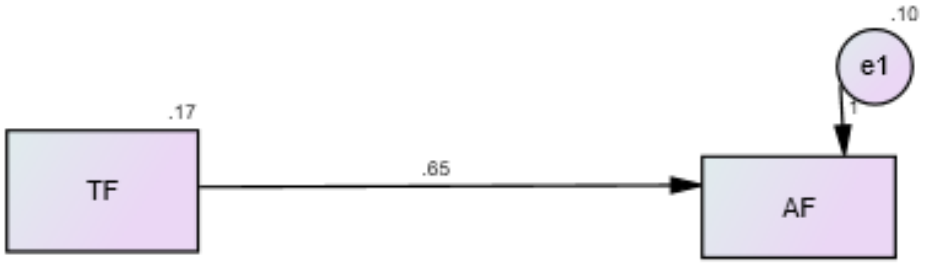


FIGURE 4.5: Direct Effect between Independent and Dependent Variables

After adding a mediator, the changes are noted in the relations of direct, and indirect mediating variables. The yellow highlighted value in Figure 4.6 shows the direct relationship between independent and dependent variables, which is reduced from 0.65 to 0.36 due to the addition of a mediator variable. The indirect effect is highlighted with green color as it connects the independent variable to the mediator (having a value of 0.51) and interlinks the mediator to the dependent variable with a value of 0.57. It can be observed that after adding a mediator, the direct effect is reduced as the indirect and mediator effects become significant in the model.

There is a significant relation exists among all of the three variables as shown by the p (***) in Figure 4.9.

Hence, it can be inferred that there exists a significant relation in both the direct and indirect effects of all three variables and the value of the direct relation is not very low, so a partial mediation occurs in the model. Standardized indirect effects are also checked through two-tailed significance and the value is less than 0.05, proving that there is a mediation effect in the model. Based on both mediation analysis results, it is concluded that Hypothesis 2 is accepted.

Hence, it is also concluded that there is a significant relation in both the direct and indirect effects of all three factors and the value of the direct relation is not very low, so partial mediation occurred in our model. Standardized indirect effects are also checked through two-tailed significance in figure 4.8 and the value is less than 0.05 which also proves there is a mediation effect in the model. After analysis of mediation, it is concluded from the result that hypothesis 2 is accepted.

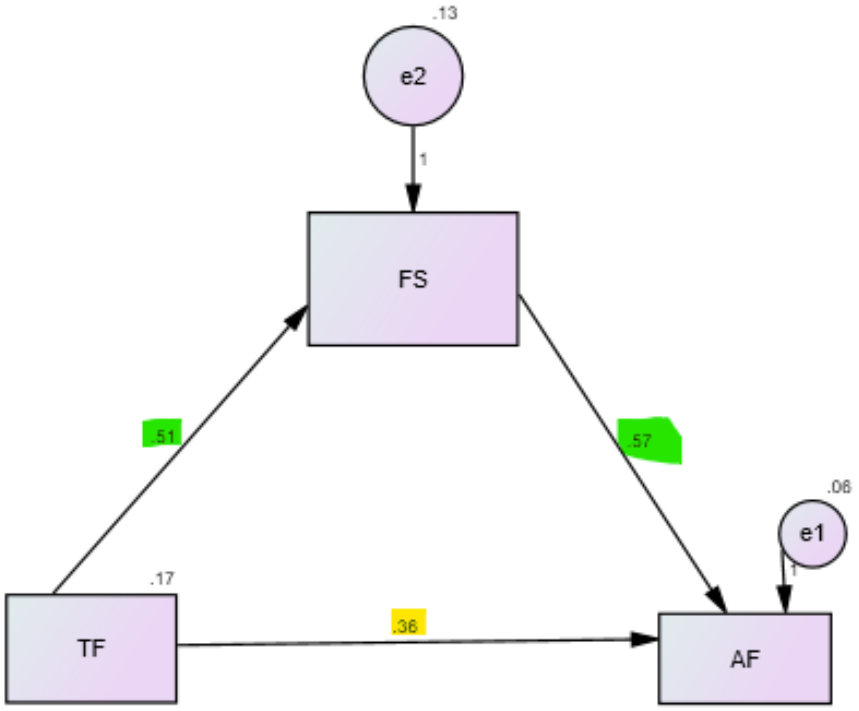


FIGURE 4.6: Direct and Indirect Effect Among Independent and Dependent Variables Through a Mediator

Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
FS	<---	TF	.512	.048	10.659	***	
AF	<---	TF	.361	.040	9.057	***	
AF	<---	FS	.570	.040	14.310	***	

FIGURE 4.7: Representation of Significance Relation of all Variables

Standardized Indirect Effects - Two Tailed Significance (BC) (Group number 1 - Default model)

	TF	FS
FS	...	...
AF	.001	...

FIGURE 4.8: Check the Two-Tailed Significance Relation

4.9 Moderation Analysis

Moderation analysis defines the relationship between independent and dependent variables that will change according to the moderator variable [109]. The relationship direction and strength among the two variables are dependent on the moderator as the moderator operates the independent and dependent variables. Memon et al. [110] reported that the moderation variable tells "when and how" the relationship between both variables changes concerning different contexts and conditions for deep interaction of the research model mechanism. Additionally, selected moderating variables become essential that assess the relationship between two variables with the same apprehensions.

In the current research work, two ways are used to analyze the moderation direction and strength effect of the independent and dependent variables. One way is through SPSS software with the plug-in of Process by Andrew F. Hayes and model 1 is used for the moderation process. The second way is through the AMOS module to analyze the moderation effect and significance of variables.

4.9.1 Moderation Analysis through SPSS Software

It is assumed that the technology acceptance model (TAM) acts as a beneficial moderator between technical and administrative factors for technology adoption in an organization.

The first task is to analyze whether the technical and administrative factors are linked with TAM in different ways. The value of R-square is equal to 0.7430, which indicates that a change of one unit in the technology acceptance model causes an increase of 0.7430 units in the technical factors. After that, the p-value is less than 0.05, which shows that the link between administrative and technical factors is enormously modest and significant. Model 1 is shown for moderation analysis and process macros of SPSS are used to perform the analysis with confidence as an output. The lower and higher confidence intervals have the values 0.1204 and 0.2449, respectively for the interaction term (TF*TAM). There is no zero in the range of these values as both have the same sign. The conditional effect of the

```
Model  : 1
    Y  : AF
    X  : TF
    W  : TAM

Sample Size:  322
OUTCOME VARIABLE:
 AF
Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .8620       .7430      .2383   306.4800     3.0000   318.0000      .0000
Model
             coeff         se          t          p       LLCI       ULCI
constant      .8085      .2043     3.9577      .0001      .4065     1.2104
TF            .1493      .0954     1.5651      .1186     -.0384      .3370
TAM          -.0595      .0992     2.5994      .0493     -.2546      .1357
Int_1         .1827      .0316     2.7750      .0120      .1204      .2449

Product terms key:
 Int_1    :        TF       x        TAM

Test(s) of highest order unconditional interaction(s):
       R2-chng          F        df1        df2          p
X*W      .0270    33.3503     1.0000   318.0000      .0120
----------
    Focal predict: TF      (X)
          Mod var: TAM     (W)
Conditional effects of the focal predictor at values of the moderator(s):

        TAM     Effect         se          t          p       LLCI       ULCI
     1.6000      .4416      .0620     7.1259      .0000      .3197      .5635
     2.4000      .5877      .0560    10.5020      .0000      .4776      .6978
     3.2000      .7339      .0609    12.0574      .0000      .6141      .8536
```

FIGURE 4.9: Moderation Analysis through SPSS Software

focal predictor moderator shows that as the values increase, the parallel consequent values are also increased. Therefore, it can be said that by adding a moderator the effect on the independent and dependent variables is increased.

The results presented in Table 4.8 exhibit that there is a significant relation and 74% of changes occur in the variables if the moderator is changed. Since LLCI and ULCI both are positive values, which means that moderation has occurred in the model. If one value is positive and the other is negative then moderation does not occur.

TABLE 4.8: SPSS Moderation Results

Interaction-terms	**R-change**	**R- square**	**LLCI**	**ULCI**
TF*TAM	0.8620	0.7430	0.1204	0.2449

***LLCI: lower limit confidence interval

***UCLI: Upper limit confidence interval

Figure 5.1 below shows the graphical trends of moderation results defined with slope steepness. The graph line with a low level of TAM is much steeper as compared to the high-level TAM line, this means that if low TAM is applied in an organization, it will make a stronger relationship between TF and AF. Due to the steepness in low-level TAM the relationship between TF and AF is stronger as compared to high-level TAM. However, at a high level of TAM, the line trend shows straightened, this means that at a high level of TAM, the increase in TF does not lead to similar change in AF so in conclusion high-level TAM weakness the relationship between TF and AF. During the literature review, it was identified that a higher value of TAM along with high TF causes to increase AF variable and vice versa. In the future, the line steepness may be analyzed with more responses and other population samples. If lines are parallel to each other without any steepness, then it can be said that there is no moderation taking place among the variables. Hence, from the graph of moderation, it can be noted that there is a strong moderation relation among the variables because lines are not parallel and they get steeper at the end, so moderation exists in the research model variables.

4.9.2 Moderation Analysis through AMOS Module

The relationship between independent and dependent variables is analyzed whether it is strong or weak due to the moderator. The moderation in the AMOS module is performed in two ways; categorical moderator and metric moderator. In the current work, the metric moderator is used to analyze the results [111]. Three steps are followed for metric moderator analysis; the first one is Zscore, in which R parameters are calculated, the second is interaction, in which effects are analyzed, and the third step is to conclude hierarchical regression.

Figure 4.11 shows that by adding a moderator the relation between independent and dependent variables increases. There is a strong moderation effect in the research model and exhibits that TAM addition has a significant effect on other variables.

Zscore (TF)= standardized values as an independent variable

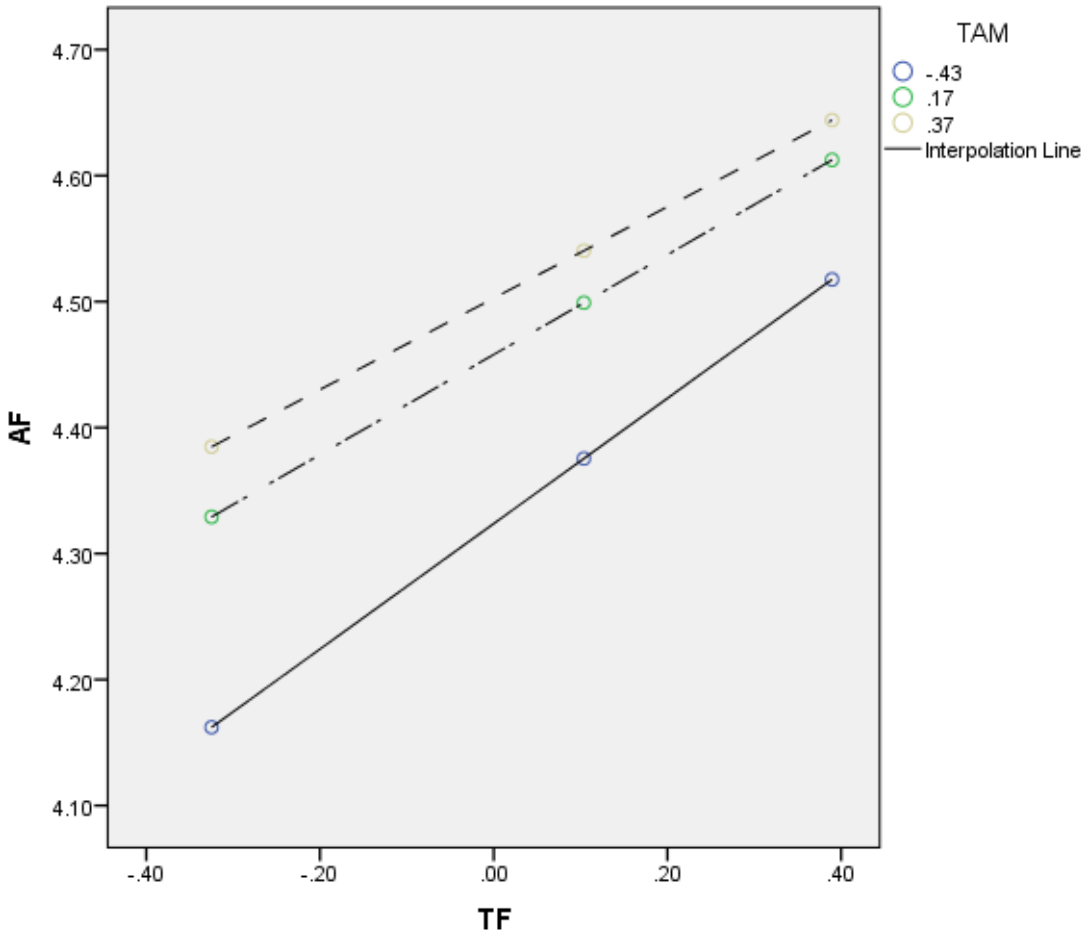


FIGURE 4.10: Graphical Trends of Moderation Analysis

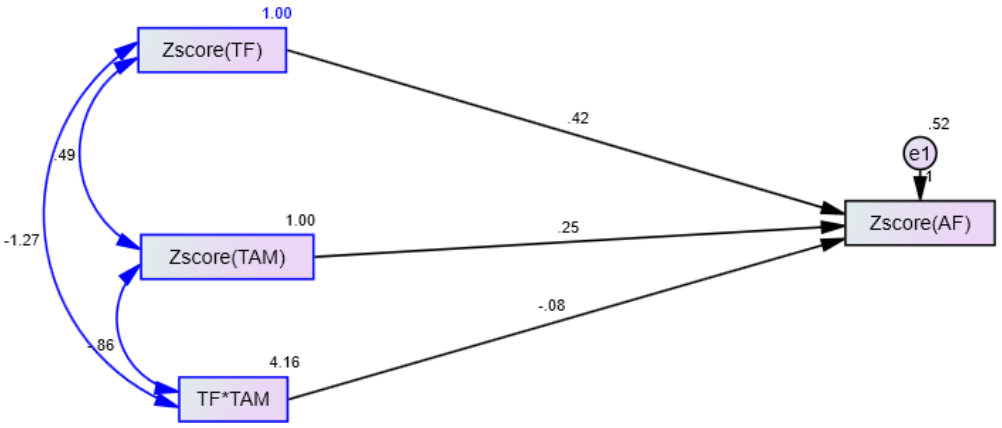


FIGURE 4.11: Moderation Analysis Results in AMOS Module

Zscore (TAM)= standardized values as moderator variable

Zscore (AF)= standardized values as a dependent variable

TF*TAM (moderator)= Interaction variable

Figure 4.12 displays the significance of regression weights, variances, and covariances. The moderator is significant as p values are less than 0.05, which means that significance has occurred in the research model. It simply describes that by adding a moderator between independent and dependent variables, strong moderation occurred as it did not become insignificant for the research model. Due to this, it can be inferred that the addition of a moderator increases the effect on the independent and dependent variables. Based on the results of moderation analysis, Hypothesis 3 "the technology acceptance model (TAM) moderates the relationship between technical factors (TF) and administrative factors (AF)" is accepted.

Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
ZAF	<---	ZTF	.416	.054	7.677	***	
ZAF	<---	ZTAM	.253	.047	5.426	***	
ZAF	<---	moderator1	-.078	.026	-3.070	.002	

Covariances: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
ZTF	<-->	ZTAM	.485	.062	7.839	***	
ZTF	<-->	moderator1	-1.273	.134	-9.496	***	
ZTAM	<-->	moderator1	-.864	.123	-6.995	***	

Variances: (Group number 1 - Default model)

	Estimate	S.E.	C.R.	P	Label
ZTF	.997	.079	12.669	***	
ZTAM	.997	.079	12.669	***	
moderator1	4.160	.328	12.669	***	
e1	.516	.041	12.669	***	

FIGURE 4.12: Test for Significance of Relation among Variable

4.10 Confirmatory Factors Analysis (CFA)

Confirmatory factors analysis (CFA) is known as the statistical method that assesses the model fitness through the connection of observable variables in the model. This practice is frequently used with structural equation modeling (SEM) and it is used to scrutinize the hypothesized correlation among observable variables [112]. To apply To apply CFA to the model, researchers need to identify the components with their predicted correlations. The CFA is used to determine the indicators (observed variables) accurately to reflect the constructs (latent variables) that are measured in the model. Data evaluation is performed in such a way that how closely the variables are interlinked with each other. The sufficiency of observed variables is analyzed with the hypothesized relationship. Every variable dependency concept is employed through the validation of CFA and demonstrates the best match of the model. No single model is accurate or deemed to be the best that describes the completed fitness and effectiveness of the model. Disagreements are still surrounded everywhere and everyone can't rely on the calculated fit indices. However, the factors are validated and convergent is assessed along with the discriminant's validity, which evaluates the measurement of the model.

The research work reported by Brown and Moore [113] defined the CFA with model fitness through different fit indices i.e. Chi-square, RMSEA (root mean square error of approximation), SRMR (standardized root mean square residual), or RMSR (Root mean square residual), p-close, GFI (goodness of fit statistics), AGFI (Adjusted goodness of fit index), NFI (Normal fit index), Chi-Square, RFI (Relative fit index), TLI (Tucker Lewis index) and CFI (comparative fit index). All these fit indices are defined individually to clarify the concept of model fitness.

4.10.1 CMIN/Df

It is the ratio of chi-square and degree of freedom that balances between model complexity and fit. This is used for the comparison between predicted and observed data in the complete population and estimates the differences with statistics of chi-square and degree of freedom. It provides the measurement that how properly the

proposed model fits the research data. Two categorical variables of independence are analyzed that have a quality difference between expected and actual distribution. The overall model fitness is quantified through chi-square with standardized statistics. The size divergence is assessed through the fitness of covariance and sample. For small and large sample sizes, the values of chi-square less than 5.0 are acceptable fit and less than 2.0 are good fit, respectively for appropriate results. According to our model results shown in table 4.9 CMIN/Df ratio value is 2.007 which occurred within an acceptable range.

4.10.2 RMSEA(Root Mean Square Error of Approximation)

Root means square error of approximation (RMSEA) defines the key metrics that are used for the measurement of model fitness. This is a popular fit used to provide an estimation of how well the proposed model fits with the observed data. It is adjusted for the degree of freedom as the discrepancy is taken into account for the observed covariance matrix and model implied matrix. It is a deviation that is commonly applied to measure the quality of the predictions by evaluation processes. Estimated parameters involved in the model also affect the value of the RMSEA and the variations are defined through the range measurement. RMSEA values lie in the range of 0-1 and low values indicate a better fit. The range 0.05-0.08 specifies reasonable model fit while the 0.08-0.10 range indicates moderate effect and values less than 0.05 are strong/close fit in the model fit measurement. The values above 0.1 are considered a poor fit. It is required to consider other fit indices in combination with RMSEA for a more comprehensive assessment of model fit. According to our model results shown in table 4.9 RMSEA value is 0.061 which occurred within an acceptable range.

4.10.3 CFI (Comparative Fit Index)

In the comparative fit index (CFI), the comparison is performed among observed and implied covariance matrices in the model. All of the values higher than 0.9

show a good match and the value of 1 is a perfect fit match between the data and model. It is less sensitive to the sample size and superior to NFI (normal fit index) because it is more robust and generates better results. According to our model results shown in table 4.9 CFI value is 0.900 which occurred within an acceptable range.

4.10.4 NFI (Normal Fit Index)

This shows the measurement of SEM, which fits the data with the discrepancy between the hypothesized model and the chi-square value. A value near 1 is considered a good value for the model fitness. NFI shows the difference between GFI and AGFI as it is not suggested for the small sample size. If the value of NFI is higher than 1, it means that some issue occurs and it is not comprehensible; therefore, the value must be varied between 0.8 and 0.95 for a better fit. According to our model results shown in table 4.9 NFI value is 0.821 which occurred within an acceptable range.

4.10.5 IFI (Incremental Fit Index)

This calculates the frequency difference between the observed and predicate sample sizes and examines the observed data representation concerning the hypothesized distribution. It is an alternative to the chi-square test and calculates the variance relation with population covariance. In a case where the sample size is exaggerated in the chi-square test, then IFI is used to determine the model fitness. IFI acceptable value should be 0.90 or higher but closer values are also acceptable in most of the cases. According to our model results shown in table 4.9 IFI value is 0.901 which occurred within an acceptable range.

4.10.6 TLI (Tucker Lewis Index)

It is commonly known as a non-normed fit index that is used in covariance structure modeling and linear mean. The range of TLI lies between 0-1 and values must

be greater than 0.90 for good model fit indices. CFI is always greater than TLI and used in prevention research for EFA as it is highly dependent on conventional cutoff values for continuous data. According to our model results shown in table 4.9 TLI value is 0.889 which occurred within an acceptable range.

The main aim of using statistical tools is to measure as well as test the model fitness related to the given data. For this purpose, the data is opened in an Excel sheet and after that, it is converted into numbers by giving numeric values to all variables. The male is represented as 1 and the female as 2 for a clear representation of the data. After assigning numbers to all data, the saved file is open in SPSS with all constructs involved in the study work. Firm size (FS), administrative factors (AF), technical factors (TF), and technology acceptance model (TAM) have 8, 9, 7, and 5 constructs/elements, respectively.

The analysis is conducted through SPSS by selecting all the factors/variables (FS, TF, AF, and TAM).

4.11 Model Variables

4.11.1 Independent Variable (Technical factors)

The technical factor is designated as an independent variable in the model, which contains 7 sub-factors/constructs.

4.11.2 Dependent Variable (Administrative factors)

The administrative factor is set as the dependent variable in the model, which contains 9 sub-factors.

4.11.3 Mediator Variable (Firm Size)

Firm size is selected as the mediator in the model and it contains 8 sub-factors.

4.11.4 Moderator Variable (Technology Acceptance Model)

The technology acceptance model is set as the moderator in the model, which contains 5 sub-factors.

The coefficient display format is chosen and the two main options are sorted through size and suppressed small coefficients that are set with an absolute value below 0.20. To analyze whether the model is significant or not, it is checked that the confidence interval is equal to 95%, which is 0.000, the degree of freedom is 293, and the chi-square value is 3484.355. The file is saved for future changes if it is required for analysis of data. After these values, the AMOS module is launched and then the SPSS file is opened to generate the CFA model with relevant data. The CFI and RMSEA values of the CFA model are 0.900 and 0.061, respectively and these values lie within an acceptance range. Model fit indices are used to analyze and test the model fitness that determines the model analysis for an assumption result. The model fitness values of CFA are shown in Table 4.9.

In this research work, these model values are significant and these are appropriate results for further analysis.

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	84	588.047	293	.000	2.007
Saturated model	377	.000	0		
Independence model	52	3277.689	325	.000	10.085

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	.821	.801	.901	.889	.900
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

RMSEA

Model	RMSEA	LO 90	HI 90	P-CLOSE
Default model	.061	.054	.068	.000
Independence model	.183	.177	.188	.000

FIGURE 4.13: CFA Model Fit Values

Figure 4.14 describes the complete CFA model for the current research study. It indicates the results of the CFA analyses that are performed in AMOS to check

Table 4.9: Model Fit Indices

Model	Variables	RMSEA	CMIN /DF	NFI	CFI	TLI	IFI
Hypothesized Model	04	0.061	2.007	0.821	0.900	0.889	0.901

the model fitness. All values between latent and unobserved variables are less than 1, which represents that the values are true. Usually, the un-standardized estimations are not reported in AMOS because the values that occurred in it are also included in the standardized estimation. All p values in un-standardized estimates are known as standardized estimates. All of the values shown in latent variables are endogenous values for R-square in the model. So, all results shown in the model proved that the model is acceptable because all values remain in the acceptable ranges of model fitness indices.

4.12 Relations of Research Model Factors

4.12.1 Relation between Technical Factors and Administrative Factors (Hypothesis 1)

Technical and administrative are two main critical factors studied in the adoption of cyber-security locks technology for various organizations. Technical factors are linked with the privacy and security of the technology that generates specific intentions for the users and organizations. Administrative factors are linked with managerial activities in any organization and embrace technology adoption solutions in multifaceted and complicated ways. According to the literature findings, if there are positive technical factors, administrative factors are likely to apply to adopting cyber-security locks. Positive opinions related to technical factors are important as they motivate the administration on personal preferences. The negative opinions about technical factors discourage the administration and the technology adoption goal or intent is disturbed. At the same time, if technical factors are positive then administrative factors are likely to improve with the adoption

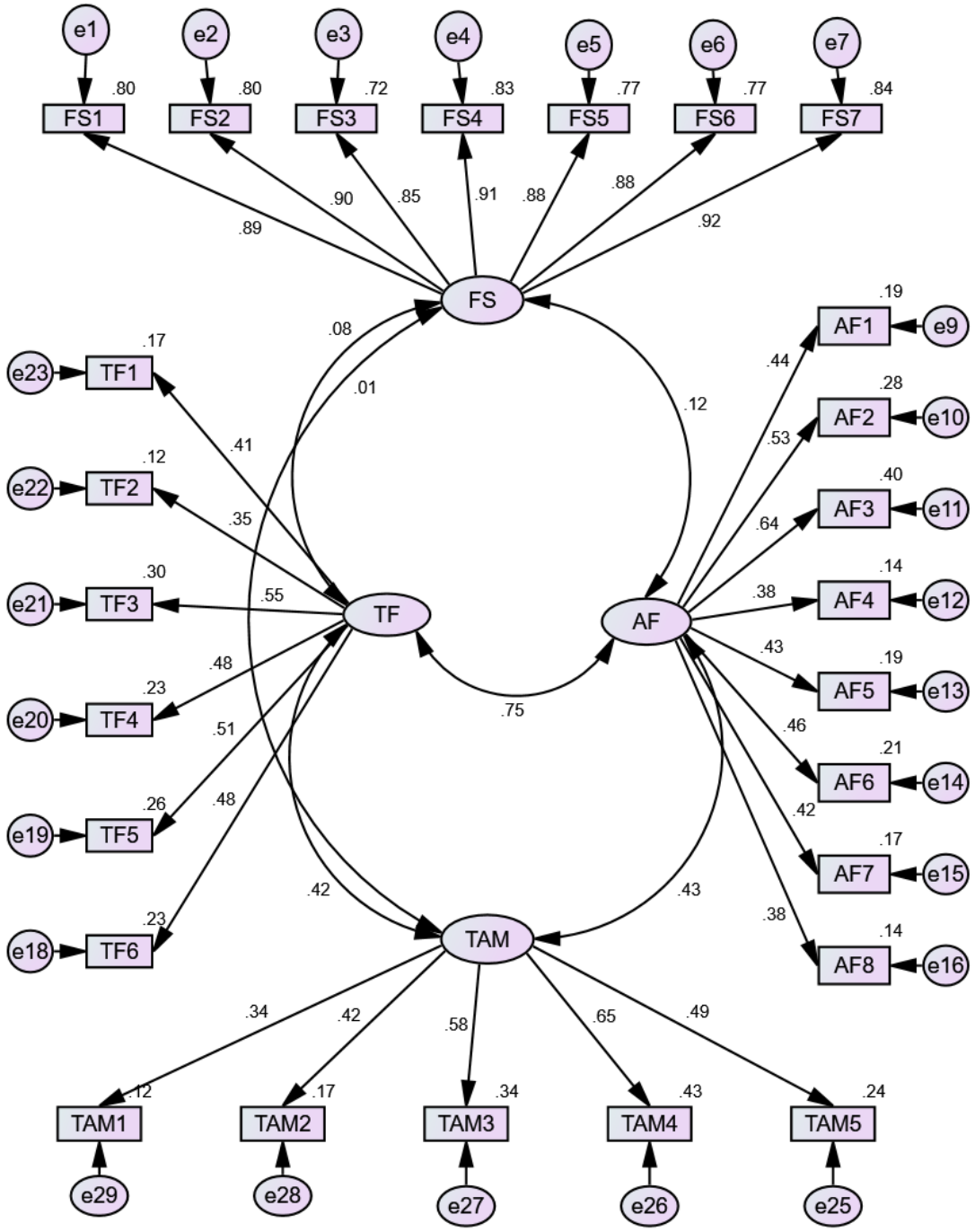


FIGURE 4.14: CFA analysis results

of technology and its solutions. If technical factors have positive output, then automatically administrative factors are increased towards the adoption of cyber-security locks in an organization due to their positive relationship. Therefore, the main aim is to increase technical awareness about cyber-security locks technology as it provides favorable solutions with numerous benefits to any organization. According to the current work, if there is a positive output of technical factors

then administrative factors are improved and the adoption of cyber-security locks prediction is embraced with advanced solutions. This emphasizes the significance of both factors in the adoption and implementation of cyber-security locks technology for an organization. The current work is moderately compatible with past research work as shown in the results of correlation and regression test analyses (beta = 0.818).

4.12.2 Mediation Role of Firm Size between Technical Factors and Administrative Factors (Hypothesis 2)

The firm size acts as a mediator among both technical and administrative factors and plays a neutral role in negotiating matters. The indirect effect of technical factors and administrative factors occurred due to firm size and changes occurred in both factors due to mediator. Firm size's main concern studied in past literature work is that it is linked with the size of an organization and firm revenues/sales. So, large organizations pay more attention to cyber-security locks adoption due to more technical expertise as compared to small organizations. Similarly, more managerial skills are available in large organizations, so the firm size becomes important in the adoption of cyber-security locks. Organizations with more sales/revenues pay more attention to new technologies and effectively manage the technical aspects of the technology with their workforce. As communicated in the past literature, the results of the current research work are also consistent and verified that firm size plays a mediating role between the technical and administrative factors of an organization. This is also proven by mediation test results that firm size mediates both the variables in an organization.

4.12.3 A Moderator Role of the Technology Acceptance Model between Technical Factors and Administrative Factors (Hypothesis 3)

The technology acceptance model (TAM) is an information system in the field of technology to predict the behavior of users towards the technology. Users may

be customers and employees when an organization uses the technology after its adoption. Perceived usefulness and perceived ease of use determinants are used to analyze the intention of employees towards the technology. After assessing both factors, it can analyze the employee's intentions individually toward the new technology and help out in the implementation of new technology. The user's attitude is very important as it refers to the positive or negative feelings of behavior towards new technology. The amount of internalized reactions and judgments related to cyber-security locks technology by every individual user is involved directly. The beliefs of the users towards the behavior of technology are based on the perceived opinions that affect the values of the culture and society. A series of propositions predict the characteristics with structural means and facilitate the basic framework to address dimensions under two sets of variables (technical and administrative factors). This is the belief of an individual user that can be linked to the ability for successful behavior and tasks. Past success can be affected by similar tasks along with time and resources. It is important to predict the behavior related to the users of cyber-security locks and make it a good influencer that beneficially works in an organization. This theory in reality applied in the current research work for user behavior analysis for the complete organizational structure to adopt cyber-security locks technology. From moderation analysis, it is found that the technology acceptance model moderates the technical factors and administrative factors. Therefore, it can be concluded that adding a moderator positively increases both the independent (technical factors) and dependent (administrative factors) variables of the model.

4.13 Summary of Accepted and Rejected Hypotheses

The acceptance and rejection decisions of the hypotheses are undertaken after testing processes. The responses are collected through a questionnaire designed according to the formulated hypotheses. Different tests are performed in SPSS and AMOS software that are concerned with the statements of the hypotheses.

Based on the test results, decisions on the hypotheses statements were undertaken and it confirmed that all the hypotheses are true and accepted.

H1: Technical factors (TF) have a positive and significant relationship with administrative factors (AF). **(ACCEPTED)**

H2: Firm size (FS) significantly mediates the relationship between technical and administrative factors (TF and AF). **(ACCEPTED)**

H3: Technical and administrative factors (TF and AF) moderate significantly with the technology acceptance model (TAM). **(ACCEPTED)**

Chapter 5

Conclusions and Recommendations

This is the final section of the research work that involves a description of the research outcomes and conclusions. Thorough insight related to the current research work and recommendations for future work are outlined. Furthermore, theoretical implications, strengths, limitations, and suggestions are demonstrated in detail.

5.1 Strength of the Research

This research employed technical and organizational factors that were determined from different aspects. Firm size is explained in terms of revenues and the size of an organization that plays a crucial role in understanding the technology adoption factors. In this study, the user behavior is analyzed through the TAM variable for a better understanding of the response toward cyber-lock adoption aspects. The characteristics of technical factors and administrative factors of an organization are combined and examined statistically to provide confident and substantial association in the study. This study integrates different factors involved in cyber-security locks adoption and highlights the use of technology for better implementation of solutions. TAM provides the framework to study different variables that impact

cyber-lock technology adoption and may be used to enhance and drive intervention in technology adoption. The confirmatory factors analysis (CFA) is used to test and recognize complex and casual relationships among different variables for deep understanding.

A consistent drive in the field of cyber-security exists worldwide and the current research work of cyber-security locks adoption in organizations is particularly contemporary and relevant. Mostly security-related decisions are made at the managerial level in response to what kind of protocols and systems should be designed for an organization. The findings of this study have significant theoretical implications for deep understating of different factors at the organizational level that influence the adoption of cyber-security locks. This helps in the development of programs and policies in an organization to increase the technology adoption of cyber-security locks with advanced solutions. The current study has attempted to establish each component measurement that enhances the reliability and validity of the data. Therefore, this work is arranged in a clear as well as precise way and the results are easily understandable to the readers.

5.2 Limitations of Research

There are several limitations of the current research work as a result of deadlines and limited resources. The access to security-sensitive organizations has always been quite difficult worldwide due to which data collection and observations become barriers owing to the sensitive security concerns. Every organization has a different culture in security terms, so relating everyone with a central point is a difficult task. Many problems were encountered in the data collection procedure while considering the convenience of the concerned respondents and their successful involvement in data collection. User behavior, especially in consumer cases, variation in response collection encountered relevant to cyber-lock technology in the start but after presenting a complete idea it was resolved mostly. Accessibility sampling has also become a great flaw in existing research work. Due to time constraints, it becomes unfeasible to gather data from a complete population, so

choosing a sample has generalizability. Through the convenience sampling approach, the complete data is gathered and the results are compiled by different means.

Finally, the thesis may come across the limitations associated with the time constraints and the diverse nature of security-sensitive organizations. Cyber-security technology risks may change rapidly due to unexpected attacks, market instability, regulatory policies and fluctuations, and other internal factors of an organization. Due to the laborious research progression, the decisions drawn from the analysis may not completely seize the real-time dynamics of security-sensitive organizations, which may confine the practical applicability of the research outcomes. Even though, this research work offers valuable insight into the cyber-security locks adoptions in the field of cyber-security. Thus, the above-mentioned limits should be recognized to confirm the stability and precise clarification of the findings.

5.3 Evaluation of Sub-Factors Significance Level

After a complete analysis of sub-factors that are derived from model factors evaluation is performed and categorize which sub-factor is highly significant, moderately significant, and significant. All of the sub-factors that occurred in different significant ranges are described in table 5.1 further down:

5.4 Conclusions

The research work integrates four main (technical, administrative, firm size, and technology acceptance model) factors related to cyber-security locks technology adoption in an organization. Primary data is gathered through questionnaires and after that, the obtained responses are used for different analyses. In this regard, SPSS software is used to analyze the model for various tests, and confirmatory factors analysis (CFA) is performed in AMOS to analyze model fitness suitably. The main conclusion derived from the analysis is that the TAM controls the technical and administrative factors of cyber-lock technology adoption for an organization.

TABLE 5.1: Evaluation of Sub-Factors Significance Level

Significance Level	Range	Sub-factors
Highly-Significant	0.70-0.99	Revenues, Resources/Assets, Market Shares, Customer Demands, Capital labor ratio, Productivity, Number of Employees.
Moderately-Significant	0.40-0.69	Top-level management, Effective communication, Training programs, and awareness campaigns, allocation of adequate resources and budget, perceived reliability and effectiveness.
Significant	0.1-0.39	Resources availability, the culture of an organization, Perceived reliability and effectiveness, potential risks, and vulnerabilities.

Whenever a new technology is introduced, the technology acceptance model is a suitable approach to observe the progress. There is a simplification function between intent to use and usage to overwhelm the barriers. Facilitation functions contain support, knowledge, training, and other belongings that help to use the technology more efficiently.

Technical factors related to technology have a positive impact as they upsurge the administration. Due to the TAM involvement, successful implementation of technology is observed with an informed decision-making process. User's positive attitude towards technology makes the use of technology easy and enhances collaboration and integration between both independent and dependent variables. Technical factors enhance effective communication and coordination with administrative factors due to direct as well as indirect relationships between them. An effective management system, operational easiness, leadership skills, transparency, and trust-building benefits make the administration more valuable. Technical factors are taken into account first in an adoption and after that, the administrative factors are considered as dependent ones under different scenarios. It is also identified that technical factors become barriers in most situations but these issues may be resolved through proper control and management at advanced levels.

All of the sub-factors occurred at different significant levels such as highly significant, moderately significant, and significant. Revenues, resources/assets, market

Shares, customer demands,capital-labor ratio, productivity, privacy and security, and number of employees all occurred in a highly significant range means these sub-factors affect more in the adoption of cyber-security locks. Top-level management, effective communication, training programs, awareness campaigns, allocation of adequate resources, and budget, all occurred in a moderately significant range means these sub-factors moderately affect the adoption of cyber-security locks. Resources availability, the culture of an organization, perceived reliability and effectiveness, potential risks, and vulnerabilities. All of these sub-factors occurred in a significant range for the adoption of cyber-security locks.

Overall, this research study provides a deep understating of influential factors for cyber-security lock adoption matters for an organization. It can help an organization devise policies and internal matters to adopt cyber-security locks technology at an advanced level by conducting awareness programs within an organization. It is necessary to note that the findings of this study are limited to the selected sample size. Further work may be conducted on this topic in varied situations and cultures to validate the findings and broaden the applicability.

5.5 Recommendations

Different recommendations based on the findings of the results and discussions to encourage the adoption of cyber-security locks technology are:

• An organization should educate employees about cyber-lock technology through awareness programs and training to obtain more benefits from this technology.

• Most users' attitudes towards the technology is positive because of its perceived usefulness and ease of use; therefore, feedback from employees should be taken from time to time about critical matters.

• During this study, it is analyzed that initial cost and privacy/security concerns are the main barriers to this technology; thus, the policies and budget management can be facilitated through vending and delayed payment services to make it affordable for small organizations as well.

• More advancement should be taken into account after the implementation of this technology in an organization as it has vast functions in combination with other technologies.

• Inter-organizational seminars may be arranged, where experts may train and provide more opportunities for users to learn from their experiences for positive advancements and solutions.

5.6 Future Research Directions

The current research work provides an efficient and reliable methodology. Future studies may be conducted with more questions on the adoption of cyber-security locks technology over numerous paths. This study has selected a sample of specific areas and geographical locations that have unique cultures as compared to other countries. These findings may or may not apply to other cultures and populations; they may vary due to users' perceptions and behaviors. For further understanding of this topic, more variables can be involved that embrace cyber-security lock adoption in different ways. In this study, the firm size acts as a mediator among technical and administrative factors, in most of the population's security matters are kept at top priority other than the revenues and sales of an organization. Some people/organizations do not make decisions based on users' perceptions, they have their policies and standards to manage the technology and they attempt to adopt it without any other involvement. More factors related to cyber-security locks technology adoption in an organization are viewed and studied for more appropriate results on larger scales. This research framework may be further extended by implementing another technology adoption theory that may provide better insights.

Bibliography

[1] Cyberlock. Cyberlock access control, 2023. Avaliable at: https://cyberlock.com/.

[2] Seungmug Zech Lee. A basic principle of physical security and its link to cybersecurity. *International Journal of Cyber Criminology*, 14(1):203–219, 2020.

[3] Grant Ho, Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song, and David Wagner. Smart locks: Lessons for securing commodity internet of things devices. In *Proceedings of the 11th ACM on Asia conference on computer and communications security*, pages 461–472, 2016.

[4] Duaa Ayesha, Tayyaba Iqbal, and Ghulam Asghar. Integration of cybersecurity locks with scada software for smart surveillance management. *Engineering Proceedings*, 45(1):17, 2023.

[5] Xiaomin Zhang, Mingyu Song, Yaohui Xu, Zhengwu Dai, and Weicong Zhang. Intelligent door lock system based on raspberry pi. In *2021 2nd International Conference on Artificial Intelligence and Information Systems*, pages 1–7, 2021.

[6] SANNE Bjartmar Hylta and PETRA SÖDERBERG. Smart locks for smart customers?: A study of the diffusion of smart locks in an urban area, 2017.

[7] Heleen Buldeo Rai, Sara Verlinde, and Cathy Macharis. Unlocking the failed delivery problem? opportunities and challenges for smart locks from a consumer perspective. *Research in Transportation Economics*, 87:100753, 2021.

[8] Zhenghao Xin, Liang Liu, and Gerhard Hancke. Aacs: Attribute-based access control mechanism for smart locks. *Symmetry*, 12(6):1050, 2020.

[9] Raihana Hassani. Security evaluation of a smart lock system, 2020.

[10] Ilkyu Ha. Security and usability improvement on a digital door lock system based on internet of things. *International journal of security and its applications*, 9(8):45–54, 2015.

[11] Muhammad Sabirin Hadis, Elyas Palantei, Amil Ahmad Ilham, and Akbar Hendra. Design of smart lock system for doors with special features using bluetooth technology. In *2018 international conference on information and communications technology (ICOIACT)*, pages 396–400. IEEE, 2018.

[12] Jeong-ile Jeong. A study on the iot based smart door lock system. In *Information Science and Applications (ICISA) 2016*, pages 1307–1318. Springer, 2016.

[13] Lucas de Camargo Silva, Mayra Samaniego, and Ralph Deters. Iot and blockchain for smart locks. In *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pages 0262–0269. IEEE, 2019.

[14] Laura Fichtner. What kind of cyber security? theorising cyber security and mapping approaches. *Internet Policy Review*, 7(2):1–19, 2018.

[15] Ameneh Seddighian Bidgoli. Cyber deviances among university students in tehran. *Journal of Culture-Communication Studies*, (Articles in Press), 2021.

[16] Marko Pavelić, Zvonimir Lončarić, Marin Vuković, and Mario Kušek. Internet of things cyber security: Smart door lock system. In *2018 international conference on smart systems and technologies (SST)*, pages 227–232. IEEE, 2018.

[17] Samiran Das and V Suresh. Configurable intelligent secures-3fa smart lock. 2019.

[18] Morched Derbali. Toward secure door lock system: Development iot smart door lock device. 2023.

[19] Luigi Aldieri and Concetto Paolo Vinci. Firm size and sustainable innovation: A theoretical and empirical analysis. *Sustainability*, 11(10):2775, 2019.

[20] Tiago Oliveira and Maria Fraga Martins. Literature review of information technology adoption models at firm level. *Electronic journal of information systems evaluation*, 14(1):pp110–121, 2011.

[21] Tobias Meyer, Heiko A von der Gracht, and Evi Hartmann. How organizations prepare for the future: a comparative study of firm size and industry. *IEEE Transactions on Engineering Management*, 69(2):511–523, 2020.

[22] Petra Andries and Ute Stephan. Environmental innovation and firm performance: How firm size and motives matter. *Sustainability*, 11(13):3585, 2019.

[23] Woon-Leong Lin, Jun-Hwa Cheah, Mohamed Azali, Jo Ann Ho, and Nick Yip. Does firm size matter? evidence on the impact of the green innovation strategy on corporate financial performance in the automotive sector. *Journal of Cleaner Production*, 229:974–988, 2019.

[24] M Hirdinis. Capital structure and firm size on firm value moderated by profitability. 2019.

[25] Thi-Hanh Vu, Van-Duy Nguyen, Manh-Tung Ho, and Quan-Hoang Vuong. Determinants of vietnamese listed firm performance: Competition, wage, ceo, firm size, age, and international trade. *Journal of Risk and Financial Management*, 12(2):62, 2019.

[26] Lailah Fujianti and Indra Satria. Firm size, profitability, leverage as determinants of audit report lag: Evidence from indonesia. *International Journal of Financial Research*, 11(2):61–67, 2020.

[27] Myung Joong Kwon and Paul Stoneman. The impact of technology adoption on firm productivity. *Economics of Innovation and New Technology*, 3(3-4):219–234, 1995.

[28] Monika Lakhwani, Omkar Dastane, Nurhizam Safie Mohd Satar, and Zainudin Johari. The impact of technology adoption on organizational productivity. *The Journal of Industrial Distribution & Business*, 11(4):7–18, 2020.

[29] Tesfamicheal Wossen, Tahirou Abdoulaye, Arega Alene, Pierre Nguimkeu, Shiferaw Feleke, Ismail Y Rabbi, Mekbib G Haile, and Victor Manyong. Estimating the productivity impacts of technology adoption in the presence of misclassification. *American Journal of Agricultural Economics*, 101(1):1–16, 2019.

[30] Maryellen R Kelley and Susan Helper. Firm size and capabilities, regional agglomeration, and the adoption of new technology. *Economics of Innovation and New technology*, 8(1-2):79–103, 1999.

[31] Thora Knight, Xiaojun Yuan, and DeeDee Bennett Gayle. Illuminating privacy and security concerns in older adults' technology adoption. *Work, Aging and Retirement*, page waac032, 2022.

[32] Kristen L Walker, Kiya Bodendorf, Tina Kiesler, Georgie de Mattos, Mark Rostom, and Amr Elkordy. Compulsory technology adoption and adaptation in education: A looming student privacy problem. *Journal of Consumer Affairs*, 57(1):445–478, 2023.

[33] Tahereh Hasani, Davar Rezania, Nadège Levallet, Norman O'Reilly, and Mohammad Mohammadi. Privacy enhancing technology adoption and its impact on smes' performance. *International Journal of Engineering Business Management*, 15:18479790231172874, 2023.

[34] Yong Liu, Jorge Ruiz-Menjivar, Lu Zhang, Junbiao Zhang, and Marilyn E Swisher. Technical training and rice farmers' adoption of low-carbon management practices: the case of soil testing and formulated fertilization technologies in hubei, china. *Journal of Cleaner Production*, 226:454–462, 2019.

[35] Satish Nambisan and Yu-Ming Wang. Technical opinion: Roadblocks to web technology adoption? *Communications of the ACM*, 42(1):98–101, 1999.

[36] Ulf Andersson, Ángels Dasí, Ram Mudambi, and Torben Pedersen. Technology, innovation and knowledge: The importance of ideas and international connectivity. *Journal of World Business*, 51(1):153–162, 2016.

[37] Ying Qian, Yulin Fang, and Jose J Gonzalez. Managing information security risks during new technology adoption. *Computers & security*, 31(8):859–869, 2012.

[38] Daniel Boothby, Anik Dufour, and Jianmin Tang. Technology adoption, training and productivity performance. *Research Policy*, 39(5):650–661, 2010.

[39] Maurice Juma Ogada, Wilfred Nyangena, and Mahmud Yesuf. Production risk and farm technology adoption in the rain-fed semi-arid lands of kenya. *African Journal of Agricultural and Resource Economics*, 4(311-2016-5543):159–174, 2010.

[40] Marijn Janssen, Vishanth Weerakkody, Elvira Ismagilova, Uthayasankar Sivarajah, and Zahir Irani. A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. *International journal of information management*, 50:302–309, 2020.

[41] Berlilana, Tim Noparumpa, Athapol Ruangkanjanases, Taqwa Hariguna, and Sarmini. Organization benefit as an outcome of organizational security adoption: The role of cyber security readiness and technology readiness. *Sustainability*, 13(24):13761, 2021.

[42] Jinxia Jiao, ChenGuang Liu, and Yan Xu. Effects of stakeholder pressure, managerial perceptions, and resource availability on sustainable operations adoption. *Business strategy and the environment*, 29(8):3246–3260, 2020.

[43] Jim Witschey, Shundan Xiao, and Emerson Murphy-Hill. Technical and personal factors influencing developers' adoption of security tools. In *Proceedings of the 2014 ACM Workshop on Security Information Workers*, pages 23–26, 2014.

[44] Tugrul Daim, Nuri Basoglu, and Ilda Tanoglu. A critical assessment of information technology adoption: technical, organisational and personal perspectives. *International Journal of Business Information Systems*, 6(3):315–335, 2010.

[45] Mohammed Saeed A Alqahtani and Eila Erfani. Exploring the relationship between technology adoption and cyber security compliance: A quantitative study of utaut2 model. *International Journal of Electronic Government Research (IJEGR)*, 17(4):40–62, 2021.

[46] Inge van de Weerd, Ivonne Sartika Mangula, and Sjaak Brinkkemper. Adoption of software as a service in indonesia: Examining the influence of organizational factors. *Information & Management*, 53(7):915–928, 2016.

[47] Miftachul Huda. Empowering application strategy in the technology adoption: insights from professional and ethical engagement. *Journal of Science and Technology Policy Management*, 10(1):172–192, 2019.

[48] James E Smith and Canan Ulu. Technology adoption with uncertain future costs and quality. *Operations Research*, 60(2):262–274, 2012.

[49] Hülya Ünlü and Ali Saleh Alshebami. Source of fund, financial constraints, political instability, and firm innovation: empirical evidence from arab spring countries. *Journal of Sustainable Finance & Investment*, 12(1):195–213, 2022.

[50] Ali Al Hadwer, Madjid Tavana, Dan Gillis, and Davar Rezania. A systematic review of organizational factors impacting cloud-based technology adoption using technology-organization-environment framework. *Internet of Things*, 15:100407, 2021.

[51] Arega Shumetie and Mulugeta Damie Watabaji. Effect of corruption and political instability on enterprises' innovativeness in ethiopia: pooled data based. *Journal of Innovation and Entrepreneurship*, 8(1):1–19, 2019.

[52] Ganesh Kumar, Carole Engle, and Craig Tucker. Factors driving aquaculture technology adoption. *Journal of the world aquaculture society*, 49(3):447–476, 2018.

[53] Anupam B Jena and Tomas J Philipson. Endogenous cost-effectiveness analysis and health care technology adoption. *Journal of health economics*, 32(1):172–180, 2013.

[54] Dursun Barrios, Fernando José Restrepo-Escobar, and Mario Cerón-Muñoz. Factors associated with the technology adoption in dairy agribusiness. *Revista facultad nacional de agronomía Medellin*, 73(2):9221–9226, 2020.

[55] Mehdi Moradi and Ehsan Rahmani Nia. The impact of organizational factors based on technology-organization-environment (toe) framework on practical levels and characteristics of audit analysis and internal audit performance. *European Journal of Business and Management Research*, 5(4), 2020.

[56] Ampadu Seth, A John Coffie, Amoako Richard, and SA Stephen. Hospital administration management technology adoption: a theoretical test of technology acceptance model and theory of planned behavior on hamt adoption. *American Journal of Public Health Research*, 7(1):21–26, 2019.

[57] Chukwuma Nnaji, John Gambatese, Ali Karakhan, and Robert Osei-Kyei. Development and application of safety technology adoption decision-making tool. *Journal of construction engineering and management*, 146(4):04020028, 2020.

[58] Pierre-Andre Julien and Louis Raymond. Factors of new technology adoption in the retail sector. *Entrepreneurship theory and practice*, 18(4):79–90, 1994.

[59] Dana Rad, Anca Egerau, Alina Roman, Tiberiu Dughi, Evelina Balas, Roxana Maier, Sonia Ignat, and Gavril Rad. A preliminary investigation of the technology acceptance model (tam) in early childhood education and care. *BRAIN. Broad Research in Artificial Intelligence and Neuroscience*, 13(1):518–533, 2022.

[60] Nikola Marangunić and Andrina Granić. Technology acceptance model: a literature review from 1986 to 2013. *Universal access in the information society*, 14:81–95, 2015.

[61] Rawan Alsharida, Maytham Hammood, and Mostafa Al-Emran. Mobile learning adoption: A systematic review of the technology acceptance model

from 2017 to 2020. *International Journal of Emerging Technologies in Learning (IJET)*, 16(5):147–162, 2021.

[62] Hamaad Rafique, Alaa Omran Almagrabi, Azra Shamim, Fozia Anwar, and Ali Kashif Bashir. Investigating the acceptance of mobile library applications with an extended technology acceptance model (tam). *Computers & Education*, 145:103732, 2020.

[63] Sukendro Sukendro, Akhmad Habibi, Khaeruddin Khaeruddin, Boy Indrayana, Syahruddin Syahruddin, Fredrik Alfrets Makadada, and Hikmad Hakim. Using an extended technology acceptance model to understand students' use of e-learning during covid-19: Indonesian sport science education context. *Heliyon*, 6(11), 2020.

[64] Izra Berakon, Muhammad Ghafur Wibowo, Achmad Nurdany, and Hendy Mustiko Aji. An expansion of the technology acceptance model applied to the halal tourism sector. *Journal of Islamic Marketing*, 14(1):289–316, 2023.

[65] Ierei Park, Donggeun Kim, Jungwook Moon, Seoyong Kim, Youngcheoul Kang, and Sangseok Bae. Searching for new technology acceptance model under social context: analyzing the determinants of acceptance of intelligent information technology in digital transformation and implications for the requisites of digital sustainability. *Sustainability*, 14(1):579, 2022.

[66] Kwonsang Sohn and Ohbyung Kwon. Technology acceptance theories and factors influencing artificial intelligence-based intelligent products. *Telematics and Informatics*, 47:101324, 2020.

[67] Said A Salloum, Ahmad Qasim Mohammad Alhamad, Mostafa Al-Emran, Azza Abdel Monem, and Khaled Shaalan. Exploring students' acceptance of e-learning through the development of a comprehensive technology acceptance model. *IEEE access*, 7:128445–128462, 2019.

[68] Md Aynul Hoque, Rajah Rasiah, Fumitaka Furuoka, and Sameer Kumar. Technology adoption in the apparel industry: insight from literature review

and research directions. *Research Journal of Textile and Apparel*, 25(3):292–307, 2021.

[69] Nirmal M Menon and I Sujatha. Influence of rogers' theory of innovation of diffusion on customer's purchase intention–a case study of solar photovoltaic panels. In *IOP Conference Series: Materials Science and Engineering*, volume 1114, page 012059. IOP Publishing, 2021.

[70] Ali Junaid Khan, Waseem Ul Hameed, Jawad Iqbal, Ashfaq Ahmad Shah, Muhammad Atiq Ur Rehman Tariq, and Saira Ahmed. Adoption of sustainability innovations and environmental opinion leadership: A way to foster environmental sustainability through diffusion of innovation theory. *Sustainability*, 14(21):14547, 2022.

[71] Bryan J Hains and Kristina D Hains. Community reaction towards social innovation: A discussion of rogers' diffusion of innovations theory in consideration of community emotional response. *J. Int. Agric. Ext. Educ*, 27:34–46, 2020.

[72] Sarah Outcault, Angela Sanguinetti, and Leslie Nelson. Technology characteristics that influence adoption of residential distributed energy resources: Adapting rogers' framework. *Energy Policy*, 168:113153, 2022.

[73] Mohamed Aboelmaged. E-waste recycling behaviour: An integration of recycling habits into the theory of planned behaviour. *Journal of Cleaner Production*, 278:124182, 2021.

[74] Muhammad Zubair Alam, Shazia Kousar, and Ch Abdul Rehman. Role of entrepreneurial motivation on entrepreneurial intentions and behaviour: theory of planned behaviour extension on engineering students in pakistan. *Journal of Global Entrepreneurship Research*, 9(1):1–20, 2019.

[75] Jaap Sok, Joao Rossi Borges, Peter Schmidt, and Icek Ajzen. Farmer behaviour as reasoned action: a critical review of research with the theory of planned behaviour. *Journal of Agricultural Economics*, 72(2):388–412, 2021.

[76] Madeline Judge, Georgia Warren-Myers, and Angela Paladino. Using the theory of planned behaviour to predict intentions to purchase sustainable housing. *Journal of cleaner production*, 215:259–267, 2019.

[77] Sina Rejali, Kayvan Aghabayk, Saeed Esmaeli, and Nirajan Shiwakoti. Comparison of technology acceptance model, theory of planned behavior, and unified theory of acceptance and use of technology to assess a priori acceptance of fully automated vehicles. *Transportation research part A: policy and practice*, 168:103565, 2023.

[78] Eddie WL Cheng. Choosing between the theory of planned behavior (tpb) and the technology acceptance model (tam). *Educational Technology Research and Development*, 67:21–37, 2019.

[79] S Martono, H Mukhibad, I Anisykurlillah, and A Nurkhin. Evaluation of acceptance of information systems in state university with theory of planned behavior and theory of acceptance model approaches. *Management Science Letters*, 10(14):3225–3234, 2020.

[80] Li Hua and Shanyong Wang. Antecedents of consumers' intention to purchase energy-efficient appliances: An empirical study based on the technology acceptance model and theory of planned behavior. *Sustainability*, 11(10):2994, 2019.

[81] Lai-Wan Wong, Lai-Ying Leong, Jun-Jie Hew, Garry Wei-Han Tan, and Keng-Boon Ooi. Time to seize the digital evolution: Adoption of blockchain in operations and supply chain management among malaysian smes. *International Journal of Information Management*, 52:101997, 2020.

[82] Waranpong Boonsiritomachai and Krittipat Pitchayadejanant. Determinants affecting mobile banking adoption by generation y based on the unified theory of acceptance and use of technology model modified by the technology acceptance model concept. *Kasetsart Journal of Social Sciences*, 40(2):349–358, 2019.

[83] Hans E Fischer, William J Boone, and Knut Neumann. Quantitative research designs and approaches. In *Handbook of research on science education*, pages 28–59. Routledge, 2023.

[84] Taro Yamane. Statistics: An introductory analysis. 1973.

[85] Marvin L Wolverton. Research design, hypothesis testing, and sampling. *Appraisal journal*, 77(4), 2009.

[86] Never Mujere. Sampling in research. In *Mixed methods research for improved scientific study*, pages 107–121. IGI Global, 2016.

[87] Tomoko Nemoto and David Beglar. Likert-scale questionnaires. In *JALT 2013 conference proceedings*, pages 1–8, 2014.

[88] Pooja Bhardwaj. Types of sampling in research. *Journal of Primary Care Specialties*, 5(3):157–163, 2019.

[89] W Paul Vogt, Dianne C Gardner, and Lynne M Haeffele. *When to use what research design*. Guilford Press, 2012.

[90] Julie Pallant. *SPSS survival manual: A step by step guide to data analysis using IBM SPSS*. McGraw-hill education (UK), 2020.

[91] Jitesh J Thakkar. Structural equation modelling. *Application for Research and Practice*, 2020.

[92] Rex B Kline. *Principles and practice of structural equation modeling*. Guilford publications, 2023.

[93] Joseph F Hair Jr, G Tomas M Hult, Christian M Ringle, Marko Sarstedt, Nicholas P Danks, Soumya Ray, Joseph F Hair, G Tomas M Hult, Christian M Ringle, Marko Sarstedt, et al. An introduction to structural equation modeling. *Partial least squares structural equation modeling (PLS-SEM) using R: a workbook*, pages 1–29, 2021.

[94] Peter G Smith, Richard H Morrow, and David A Ross. Preliminary studies and pilot testing. In *Field Trials of Health Interventions: A Toolbox. 3rd edition*. OUP Oxford, 2015.

[95] Mohamad Adam Bujang, Evi Diana Omar, and Nur Akmal Baharum. A review on sample size determination for cronbach's alpha test: a simple guide for researchers. *The Malaysian journal of medical sciences: MJMS*, 25(6):85, 2018.

[96] George Ursachi, Ioana Alexandra Horodnic, and Adriana Zait. How reliable are measurement scales? external factors with indirect influence on reliability estimators. *Procedia Economics and Finance*, 20:679–686, 2015.

[97] Keith S Taber. The use of cronbach's alpha when developing and reporting research instruments in science education. *Research in science education*, 48:1273–1296, 2018.

[98] Donald R Bacon, Paul L Sauer, and Murray Young. Composite reliability in structural equations modeling. *Educational and psychological measurement*, 55(3):394–406, 1995.

[99] Carl Duke, Shima Hamidi, and Reid Ewing. Validity and reliability. In *Basic Quantitative Research Methods for Urban Planners*, pages 88–106. Routledge, 2020.

[100] Philip Sedgwick. Pearson's correlation coefficient. *Bmj*, 345, 2012.

[101] Nithya J Gogtay and Urmila M Thatte. Principles of correlation analysis. *Journal of the Association of Physicians of India*, 65(3):78–81, 2017.

[102] Khushbu Kumari and Suniti Yadav. Linear regression analysis study. *Journal of the practice of Cardiovascular Sciences*, 4(1):33–36, 2018.

[103] Jeremy Arkes. *Regression analysis: a practical introduction*. Taylor & Francis, 2023.

[104] Andrew F Hayes. Process: A versatile computational tool for observed variable mediation, moderation, and conditional process modeling, 2012.

[105] Dawn Iacobucci. *Mediation analysis*. Number 156. Sage, 2008.

[106] Soleman Abu-Bader and Tiffanie Victoria Jones. Statistical mediation analysis using the sobel test and hayes spss process macro. *International Journal of Quantitative and Qualitative Research Methods*, 2021.

[107] Daniel Danner, Dirk Hagemann, and Klaus Fiedler. Mediation analysis with structural equation models: Combining theory, design, and statistics. *European Journal of Social Psychology*, 45(4):460–481, 2015.

[108] Joel Collier. *Applied structural equation modeling using AMOS: Basic to advanced techniques*. Routledge, 2020.

[109] Juan-José Igartua and Andrew F Hayes. Mediation, moderation, and conditional process analysis: Concepts, computations, and some common confusions. *The Spanish Journal of Psychology*, 24:e49, 2021.

[110] Mumtaz Ali Memon, Jun-Hwa Cheah, T Ramayah, Hiram Ting, Francis Chuah, and Tat Huei Cham. Moderation analysis: issues and guidelines. *Journal of Applied Structural Equation Modeling*, 3(1):1–11, 2019.

[111] Syed Hamad Hassan Shah, Shen Lei, Syed Talib Hussain, and Syeda Mariam. How consumer perceived ethicality influence repurchase intentions and word-of-mouth? a mediated moderation model. *Asian Journal of Business Ethics*, 9:1–21, 2020.

[112] Ilhan Koyuncu and ABDULLAH KILIÇ. The use of exploratory and confirmatory factor analyses: A document analysis. *Egitim Ve Bilim-Education and Science*, 44(198), 2019.

[113] Timothy A Brown and Michael T Moore. Confirmatory factor analysis. *Handbook of structural equation modeling*, 361:379, 2012.

Appendix

The appendix portion contains the questionnaire of the research. The collection of responses is taken out through Google Forms source and participants fill out the questionnaire online. The questionnaire contains two main sections first is related to demographics and the second section contains four variables. Variables are firm size, administrative factors, technical factors, and technology acceptance model.

Questionnaire

Firm Size:

1. The size of an organization influences the need for cyber-security locks.

o Strongly Agree o Agree o Neutral o Disagree o Strongly Disagree

2. Larger organizations are more likely to invest in cyber-security locks.

o Strongly Agree o Agree o Neutral o Disagree o Strongly Disagree

3. Smaller organizations face greater challenges in adopting cyber-security locks due to limited resources. o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

4. The revenues, assets, and resources of an organization affect its willingness to adopt cyber-security locks.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

5. The size of an organization affects market changes to handle potential cyber threats effectively.

o Strongly Agree o Agree o Neutral o Disagree o Strongly Disagree

6. The adoption of cyber-security locks is more common in organizations with a larger number of employees.

o Strongly Agree o Agree o Neutral o Disagree o Strongly Disagree

7. Large market share organizations have dedicated IT departments to manage cyber-security locks.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

8. Small productivity organizations find it more challenging to implement and maintain cyber-security locks compared to large productivity organizations.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

Administrative Factors:

9. Top-level management plays a crucial role in promoting the adoption of cyber-security locks due to its ease of integration and operability.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

10. Effective communication of an organization is important for encouraging the adoption of cyber-security locks.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree 11. Administrative support and commitment are essential for the successful implementation and maintenance of cyber-security locks.

o Strongly Agree o Agree o Neutral o Disagree o Strongly Disagree 12. The management security policies and procedures influence the adoption of cyber-security locks.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

13. Training programs and awareness campaigns contribute to the increased adoption of cyber-security locks within the organization. o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

14. Clear responsibilities and accountabilities related to cyber-security locks are defined by management.

o Strongly Agree o Agree o Neutral o Disagree o Strongly Disagree

15. The allocation of adequate resources and budget for cyber-security initiatives is prioritized by management. o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

16. The management of an organization that adopts cyber-security locks is affected by the advanced benefits.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

17. The management could promote a culture of security consciousness and encourage employees to adopt cyber-security locks.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree Technical Factors:

18. Resources availability of advanced technologies plays an independent role in the adoption of cyber-locks over an organization.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree 19. The ease of integration and operability of cyber-security locks with other security systems affects their adoption. o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

20. The perceived reliability and effectiveness of cyber-security locks impact their adoption.

o Strongly Agree o Agree o Neutral o Disagree o Strongly Disagree

21. The technical training about cyber-security locks increases the awareness about new technologies in an organization.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

22. The cost of acquiring and implementing cyber-security locks is a significant factor influencing their adoption.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

23. The compatibility of cyber-security locks with different operating systems and platforms influences their adoption.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

24. The adoption of cyber-security locks can mitigate the potential risks and vulnerabilities?

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

Technology Acceptance Model (TAM):

25. The perceived usefulness and ease of use for cyber-security locks affect technical and administrative factors within the organization.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

26. The organization believes that adopting cyber-security locks would enhance the safety and security of its equipment and assets.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

27. The organization considers the feedback and recommendations of users (employees and customers) when deciding to adopt cyber-security locks.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

28. The organization evaluates the compatibility of cyber-security locks with existing workflows and processes.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree

29. The organization conducts user training programs to facilitate the successful adoption of cyber-security locks.

o Strongly Agree o Disagree o Neutral o Agree o Strongly Disagree