

**FACTORS INFLUENCING THE ADOPTION OF
INTERNET OF THINGS FOR HOME SECURITY
IN DHAKA HOUSEHOLDS**

ARIF MAHMUD

UNIVERSITI SAINS MALAYSIA

2023

**FACTORS INFLUENCING THE ADOPTION OF
INTERNET OF THINGS FOR HOME SECURITY
IN DHAKA HOUSEHOLDS**

by

ARIF MAHMUD

**Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy**

May 2023

ACKNOWLEDGEMENT

In the beginning, I am grateful to Allah (SWT), the most gracious and merciful, for his continuous blessings, knowledge, and persistence bestowed upon me and my family throughout this wonderful and arduous PhD journey.

Ts. Dr. Mohd Heikal Husin, my supervisor, was very encouraging and supportive throughout this research. His expertise and skills never cease to surprise me. Throughout this process, Dr. Heikal aided and accompanied me in every possible way. I owe him far more than I can fully explain and extend my heartfelt gratitude and admiration. Not only for my PhD studies but also for the rest of my life, I am grateful for having such the finest supervisor, advisor, and tutor.

My heartfelt gratitude goes to my other supervisor, Ts. Dr. Mohd Najwadi Yusoff, for his helpful recommendations and suggestions for improvement on this research. I am really lucky to work with such a wonderful person who, via his in-depth knowledge, assisted me in navigating the course of this academic activity.

The motivation came from my teachers, relatives, neighbors, colleagues, students, classmates, and friends. My sincere gratitude goes to my father-in-law, mother-in-law, brother-in-law, and sister-in-law for their prayers. I am thankful to my sister, brother-in-law, niece, and nephew. I would want to express my gratitude to everyone who has helped me along this path, whether explicitly or implicitly.

Last but not the least, without the love, support, care, and inspiration of my father, mother, wife, and two daughters, I would not have achieved so far. Therefore, this thesis is dedicated to my family.

TABLE OF CONTENTS

ACKNOWLEDGEMENT	ii
TABLE OF CONTENTS	iii
LIST OF TABLES	x
LIST OF FIGURES	xii
LIST OF ABBREVIATIONS	xiii
LIST OF APPENDICES	xiv
ABSTRAK	xv
ABSTRACT	xvii
CHAPTER 1 INTRODUCTION	1
1.1 Background	1
1.1.1 Existing Burglary Activities and Their Impact on the Affected Households	1
1.1.2 The Relationships Between Security Technologies and Burglary Crimes.....	4
1.1.3 The Efficiency of Internet of Things-Based Security Devices	6
1.1.4 The Acceptance of Internet of Things-Based Security Devices	7
1.1.5 Burglary Cases in Dhaka City	8
1.2 The Motivation Behind the Research.....	10
1.3 Problem Statement	11
1.4 Research Questions	14
1.5 Research Objectives	14
1.6 Significance of the Research	14
1.7 Definition of Key Terms	16
1.8 Outlines of the Thesis Chapters	16
CHAPTER 2 LITERATURE REVIEW	17
2.1 Introduction	17

2.2	Status of Information and Communication Technology in Bangladesh.	17
2.3	Definition of the Internet of Things	19
2.4	Existing Literature on Internet of Things-Based Security Devices.....	21
2.5	Technology Adoption Models.....	25
2.5.1	Theory of Reasoned Action.....	26
2.5.1(a)	Theory of Reasoned Action and Internet of Things	27
2.5.1(b)	Limitations of the Theory of Reasoned Action	27
2.5.2	Technology Acceptance Model.....	27
2.5.2(a)	Technology Acceptance Model 2	28
2.5.2(b)	Technology Acceptance Model 3	30
2.5.2(c)	Technology Acceptance Model and Internet of Things	31
2.5.2(d)	Limitations of Technology Acceptance Model and Extensions.....	32
2.5.3	Theory of Planned Behavior.....	32
2.5.3(a)	Theory of Planned Behavior and Internet of Things	33
2.5.3(b)	Limitations of the Theory of Planned Behavior	34
2.5.4	Unified Theory of Acceptance and Use of Technology	34
2.5.4(a)	Unified Theory of Acceptance and Use of Technology 2.	36
2.5.4(b)	Unified Theory of Acceptance and Use of Technology and Internet of Things	37
2.5.4(c)	Unified Theory of Acceptance and Use of Technology 2 and Internet of Things.....	37
2.5.4(d)	Limitations of UTAUT and UTAUT 2 Models.....	38
2.5.5	Task-Technology Fit Model.....	39
2.5.5(a)	Task-Technology Fit and Internet of Things.....	40
2.5.5(b)	Limitations of the Task-Technology Fit.....	40
2.5.6	Protection Motivation Theory	41
2.5.6(a)	Protection Motivation Theory and Internet of Things.....	43

2.5.6(b)	Limitations of Protection Motivation Theory.....	43
2.6	Selecting the Appropriate Technology Adoption Model	44
2.6.1	Why Protection Motivation Theory Is Selected?	44
2.6.2	Integrating Attitude-Social Influence-Self-Efficacy Model with Protection Motivation Theory	45
2.6.3	Attitude-Social Influence-Self-Efficacy Model.....	46
2.7	Research Hypotheses.....	47
2.7.1	Perceived Severity and the Intention to Adopt IoT	47
2.7.2	Perceived Vulnerability and the Intention to Adopt IoT	48
2.7.3	Perceived Response Efficacy and the Intention to Adopt IoT.....	48
2.7.4	Response Cost and the Intention to Adopt IoT.....	49
2.7.5	Perceived Self-Efficacy and the Intention to Adopt IoT	49
2.7.6	Social Influence and the Intention to Adopt IoT	50
2.7.7	Attitude and the Intention to Adopt IoT	51
2.8	Reasons to Include Moderators	51
2.8.1	Personal Innovativeness	56
2.8.2	Perceived Trust	58
2.9	Summary of the Chapter	62
CHAPTER 3 RESEARCH METHODOLOGY		63
3.1	Introduction	63
3.2	Research Process	63
3.3	Proposed Research Model.....	64
3.4	Research Paradigm.....	66
3.5	Research Methods	67
3.6	Sampling and Data Collection.....	68
3.6.1	Sampling Techniques	69
3.6.2	Population.....	69
3.6.3	The Unit of Analysis.....	69

3.6.4	Selection of Respondents.....	70
3.6.5	Data Collection Sources	71
3.6.6	Collection of Data from the Participants	71
3.6.7	Type of Houses	73
3.6.8	Sample Size Determination	74
3.7	Development of the Research Instrument	75
3.7.1	Adaptation of Research Instrument	76
3.7.2	Pre-test of the Survey Instrument	77
3.7.3	Likert Scale Selection	81
3.7.4	Time Dimension	81
3.8	Data Preparation.....	82
3.8.1	Missing Data and Outliers	82
3.8.2	Common Method Variance	83
3.9	Data Analysis	83
3.9.1	Factor Loading.....	83
3.9.2	Multicollinearity	84
3.9.3	Internal Consistency Reliability	84
3.9.4	Convergent Validity	84
3.9.5	Discriminating Validity	85
3.9.6	Coefficient of Determination.....	86
3.9.7	Cross Validated Redundancy.....	86
3.9.8	Path Coefficient	86
3.9.9	Effect Size.....	87
3.10	Data Analysis Techniques and Tools	87
3.10.1	Structural Equation Modeling	88
3.10.2	Statistical Package for Social Science	88
3.10.3	SmartPLS.....	88

3.11	Pilot Test Process	89
3.11.1	Pilot Test Respondents	89
3.11.2	Sample Size for the Pilot Test	90
3.11.3	Demographic Profile of the Respondents	90
3.11.4	Pilot Test Results	90
3.12	List of Methods with Approaches	91
3.13	Summary of the Chapter	92
CHAPTER 4 RESULT AND ANALYSIS.....		93
4.1	Introduction	93
4.2	Data Preparation.....	93
4.2.1	Missing Data and Outliers	94
4.2.2	Common Method Variance	94
4.3	Demographic Statistics.....	94
4.4	Data Analysis	96
4.4.1	Indicator Reliability	97
4.4.2	Indicator Validity.....	97
4.4.3	Internal Consistency Reliability	98
4.4.4	Convergent Validity	98
4.4.5	Discriminant Validity	99
4.4.6	Coefficient of Determination.....	100
4.4.7	Cross Validated Redundancy.....	100
4.4.8	Path Coefficient	101
4.4.9	Hypotheses Testing.....	101
4.4.10	Effect Sizes	102
4.5	Moderation Analysis	104
4.5.1	Moderation Results of Personal Innovativeness.....	105
4.5.1(a)	Coefficient of Determination with PI as Moderator	105

4.5.1(b)	Cross Validated Redundancy with PI as Moderator.....	105
4.5.1(c)	Path Coefficient with PI as Moderator	106
4.5.1(d)	Hypotheses Testing with PI as Moderator.....	106
4.5.1(e)	Effect Sizes with PI as Moderator	108
4.5.2	Moderation Results of Perceived Trust	110
4.5.2(a)	Coefficient of Determination with PT as Moderator.....	110
4.5.2(b)	Cross Validated Redundancy with PT as Moderator.....	110
4.5.2(c)	Path Coefficient with PT as Moderator	111
4.5.2(d)	Hypotheses Testing with PT as Moderator.....	111
4.5.2(e)	Effect Sizes with PT as Moderator	113
4.6	Plot Analysis of Moderation Effect.....	114
4.6.1	Plot Analysis of Personal Innovativeness as a Moderator.....	114
4.6.2	Plot Analysis of Perceived Trust as a Moderator	115
4.7	Summary of the Chapter	117
CHAPTER 5 DISCUSSION OF RESEARCH QUESTIONS.....		118
5.1	Introduction	118
5.2	Discussion of Findings for Research Questions.....	118
5.2.1	Discussion on Research Question 1.....	118
5.2.1(a)	Discussion on Hypothesis H1	120
5.2.1(b)	Discussion on Hypothesis H2.....	121
5.2.1(c)	Discussion on Hypothesis H3	122
5.2.1(d)	Discussion on Hypothesis H4.....	123
5.2.1(e)	Discussion on Hypothesis H5.....	123
5.2.1(f)	Discussion on Hypothesis H6.....	125
5.2.1(g)	Discussion on Hypothesis H7	127
5.2.2	Discussion on Research Question 2.....	128
5.2.2(a)	Discussion on Hypothesis H1-A.....	129

5.2.2(b)	Discussion on Hypothesis H2-A.....	129
5.2.2(c)	Discussion on Hypothesis H3-A.....	130
5.2.2(d)	Discussion on Hypothesis H4-A.....	130
5.2.2(e)	Discussion on Hypothesis H5-A.....	131
5.2.2(f)	Discussion on Hypothesis H6-A.....	132
5.2.2(g)	Discussion on Hypothesis H7-A.....	132
5.2.3	Discussion on Research Question 3.....	134
5.2.3(a)	Discussion on Hypothesis H1-B.....	135
5.2.3(b)	Discussion on Hypothesis H2-B.....	136
5.2.3(c)	Discussion on Hypothesis H3-B.....	136
5.2.3(d)	Discussion on Hypothesis H4-B.....	137
5.2.3(e)	Discussion on Hypothesis H5-B.....	138
5.2.3(f)	Discussion on Hypothesis H6-B.....	138
5.2.3(g)	Discussion on Hypothesis H7-B.....	139
5.3	Summary of the Chapter	141
CHAPTER 6 RESEARCH CONCLUSION AND FUTURE WORKS.....		142
6.1	Introduction	142
6.2	Achievement of the Objectives	142
6.3	Research Contributions	143
6.4	Research Limitations and Future Works	147
6.5	Conclusion.....	148
REFERENCES.....		150
APPENDICES		
LIST OF PUBLICATIONS		

LIST OF TABLES

	Page
Table 1.1	Burglary Rate in Different Countries 2
Table 1.2	Crime Statistics of Dhaka City..... 9
Table 1.3	Definition of Key Terms 16
Table 2.1	Shipments and Market Share of Smart Home Devices..... 22
Table 2.2	Market Share and Growth Rate of Internet of Things-Enabled Security Devices 25
Table 2.3	Variance of PMT in Different Applications..... 52
Table 2.4	Variance of ASE in Different Applications 54
Table 2.5	Inconsistent Relationship Between the Constructs 55
Table 2.6	Summary of Hypotheses 60
Table 3.1	Relationships Between Research Questions and Hypotheses 66
Table 3.2	Modified Survey Questionnaires 78
Table 3.3	Summary of Validity Standards for the Measurement Model 85
Table 3.4	Summary of Validity Standards for the Structural Model 87
Table 3.5	Summary of Methodology and Respective Approaches 91
Table 4.1	Demographic Data 95
Table 4.2	Indicator Reliability 97
Table 4.3	Indicator Validity 98
Table 4.4	Internal Consistency Reliability 98
Table 4.5	Convergent Validity 99
Table 4.6	Discriminant Validity 99
Table 4.7	Coefficient of Determination 100
Table 4.8	Predictive Relevance 100

Table 4.9	Path Coefficient.....	101
Table 4.10	Hypotheses Testing Results	102
Table 4.11	Effect Sizes	103
Table 4.12	R ² with Personal Innovativeness as Moderator.....	105
Table 4.13	Q ² with Personal Innovativeness as Moderator	106
Table 4.14	Path Coefficient with Personal Innovativeness as Moderator.....	106
Table 4.15	Hypotheses Testing Results with Personal Innovativeness as Moderator.....	107
Table 4.16	Effect Sizes with Personal Innovativeness as Moderator	108
Table 4.17	R ² with Perceived Trust as a Moderator	110
Table 4.18	Q ² with Perceived Trust as Moderator	110
Table 4.19	Path Coefficient with Perceived Trust as Moderator	111
Table 4.20	Hypotheses Testing Results with Perceived Trust as Moderator.....	112
Table 4.21	Effect Sizes with Perceived Trust as Moderator	113
Table 4.22	Moderation Effect Analysis for Personal Innovativeness.....	115
Table 4.23	Moderation Effect Analysis for Perceived Trust	116
Table 5.1	First Research Question and Associated Hypotheses	119
Table 5.2	Second Research Question and Associated Hypotheses	128
Table 5.3	Third Research Question and Associated Hypotheses.....	135

LIST OF FIGURES

		Page
Figure 2.1	Smart Home Products Market in the Asia Pacific Region	21
Figure 2.2	Market of Home Security Devices by Region	23
Figure 2.3	Theory of Reasoned Action	26
Figure 2.4	Technology Acceptance Model	28
Figure 2.5	Technology Acceptance Model 2.....	29
Figure 2.6	Technology Acceptance Model 3	30
Figure 2.7	Theory of Planned Behavior	33
Figure 2.8	Unified Theory of Acceptance and Use of Technology	35
Figure 2.9	Unified Theory of Acceptance and Use of Technology 2.....	36
Figure 2.10	Task-Technology Fit.....	39
Figure 2.11	Protection Motivation Theory	41
Figure 2.12	Attitude-Social Influence-Self-Efficacy.....	46
Figure 3.1	Research Process	64
Figure 3.2	Proposed Research Model.....	65
Figure 4.1	Research Measurement Model Results from the SmartPLS Tool ...	100
Figure 4.2	Structural Model Results from SmartPLS Tool.....	103
Figure 4.3	Hypotheses Testing Results of Direct Effect	104
Figure 4.4	Structural Model Results with Personal Innovativeness as Moderator.....	109
Figure 4.5	Hypotheses Testing Results with Personal Innovativeness as Moderator.....	109
Figure 4.6	Structural Model Results with Perceived Trust as Moderator	113
Figure 4.7	Hypotheses Testing Results with Perceived Trust as Moderator.....	114

LIST OF ABBREVIATIONS

ASE	Attitude-Social Influence-Self-Efficacy
AVE	Average Variance Extracted
HBM	Health Belief Model
IoT	Internet of Things
PMT	Protection Motivation Theory
SEM	Structural Equation Modeling
SPSS	Statistics Package for Social Science
TAM	Technology Acceptance Model
TPB	Theory of Planned Behavior
TRA	Theory of Reasoned Action
TTF	Task-Technology Fit
UTAUT	Unified Theory of Acceptance and Use of Technology

LIST OF APPENDICES

APPENDIX A	REVIEW OF IOT-BASED PAPERS
APPENDIX B	PRE-TEST RESULTS
APPENDIX C	PILOT TEST QUESTIONNAIRE
APPENDIX D	PILOT TEST DEMOGRAPHIC DATA
APPENDIX E	PILOT TEST RESULTS
APPENDIX F	RESPONSE RATE
APPENDIX G	FINAL QUESTIONNAIRE
APPENDIX H	PLOT ANALYSIS OF MODERATION EFFECT

FAKTOR-FAKTOR YANG MEMPENGARUHI PENGGUNAAN INTERNET BENDA UNTUK KESELAMATAN RUMAH DALAM ISI RUMAH DHAKA

ABSTRAK

Di peringkat global, jenayah kecurian di beberapa negara dapat dikurangkan dengan menggunakan teknologi keselamatan canggih yang disokong oleh Internet Benda (IoT). Walau bagaimanapun, jenayah ini telah menimbulkan kebimbangan di kalangan penduduk di Dhaka. Walaupun pelaksanaan peraturan dan pengembangan teknologi yang sesuai dilakukan, penerapan IoT di Bangladesh tetap rendah. Oleh itu, adalah mustahak untuk menentukan faktor-faktor yang mempengaruhi niat untuk menggunakan IoT untuk keselamatan rumah. Oleh itu, Teori Motivasi Perlindungan (PMT) dan model Sikap-Pengaruh Sosial-Keberkesanan (ASE) disatukan bersama dengan dua pemboleh ubah moderat, inovasi peribadi, dan kepercayaan yang dirasakan untuk menangani objektif penyelidikan. Penyelidikan ini menerapkan pendekatan kuantitatif untuk menganalisis data utama 348 peserta tinjauan. Berdasarkan penemuan, keparahan yang dirasakan, kerentanan yang dirasakan, keberkesanan tindak balas, kos tindak balas, dan sikap adalah faktor yang mempengaruhi niat untuk mengadaptasi IoT dengan variasi 34.9%. Lebih-lebih lagi, nilai R^2 dan Q^2 masing-masing diperbaiki, kerana kemasukan inovasi peribadi dan kepercayaan yang dirasakan sebagai moderator. Inovasi peribadi secara positif menyederhanakan hubungan antara keberkesanan tindak balas – niat, dan keberkesanan diri – niat, dan secara negatif menyederhanakan hubungan niat. Selanjutnya, kepercayaan yang dirasakan secara positif menyederhanakan hubungan antara niat kerentanan yang dirasakan, dan kos tindak balas – niat, dan secara negatif menyederhanakan hubungan niat. Oleh itu, penyelidikan ini dapat menyumbang

kepada kesan sosial berikutan pengurangan jenayah kecurian di bandar Dhaka melalui penggunaan alat IoT yang diupayakan dengan ciri keselamatan.

FACTORS INFLUENCING THE ADOPTION OF INTERNET OF THINGS FOR HOME SECURITY IN DHAKA HOUSEHOLDS

ABSTRACT

Globally, burglary crimes in some countries are effectively minimized by using advanced security technology supported by the Internet of Things (IoT). However, these crimes have caused rising concerns among residents in Dhaka. Despite the implementation of appropriate rules and technology development, IoT adoption in Bangladesh remains relatively low. Therefore, it is imperative to determine the factors that influence the intention to adopt IoT for home security. Accordingly, the Protection Motivation Theory (PMT) and Attitude-Social Influence-Self-Efficacy model (ASE) are integrated along with two moderating variables, personal innovativeness, and perceived trust to address the research objectives. This research implements a quantitative approach to analyze the primary data of 348 participants. Based on the findings, perceived severity, perceived vulnerability, response efficacy, response cost, and attitude are factors that impact the intention to adopt IoT with a variance of 34.9%. Moreover, the R^2 and Q^2 are improved respectively, due to the inclusion of personal innovativeness and perceived trust as moderators. Personal innovativeness positively moderates the relationships between response efficacy–intention, and self-efficacy–intention, and negatively moderates the attitude–intention relationship. Furthermore, perceived trust positively moderates the relationships between perceived vulnerability–intention, and response cost–intention, and negatively moderates the attitude–intention relationship. Thus, this research can contribute to a social impact following the reduction of burglary crimes in Dhaka city through the use of IoT-enabled security devices.

CHAPTER 1

INTRODUCTION

1.1 Background

Criminal activity is not merely a national concern for a specific country; but it is also a global issue that is faced by almost all countries (Ahmed, 2016). Such offenses are described as violations of norms and regulations that are banned by law (Awal et al., 2016). Household burglary, for example, is defined as an illegal entry into a domestic location with the goal of stealing (Chon, 2017). Burglary, according to Kopp (2019) and Mendlein (2021), is the most detrimental crime to society and has an influence on everyone worldwide. As a result, the focus of this research is on burglary which is one of the most common crimes affecting most houses (Chon, 2017; Peeters et al., 2018).

The following topics are explored in order to obtain a thorough understanding of the target area. The current status of global burglary attempts as well as the data associated with them is investigated first. The impact of burglary on household members is the next step which leads to a link between existing security-based technologies and a decrease in burglary tendencies in some nations. Following that, the effectiveness of internet of things (IoT) supported security devices, as well as the global adoption of these devices, is depicted. In the conclusion, examples of burglary cases in Dhaka are presented.

1.1.1 Existing Burglary Activities and Their Impact on Affected Households

Burglary is one of the most common crimes in the world. To illustrate, burglary rates in Germany increase by 57.5% from 2006 to 2015 (Wollinger et al.,

2017), and around 2.1% of the households in England and Wales are found to be burglary victims during the period 2012-2013 (Tseloni et al., 2017a). In the United States, burglary is consistently one of the most challenging issues (Chastain et al., 2016). Moreover, Kopp (2019) supports the statement that burglary is noticed to increase by 8.6% during the period 2009-2014. In addition, Australia has identified 178,276 burglary victims between the years 2014 to 2019 (Manning et al., 2022). Further, in China, 17,915 cases are reported during the period from 2013 to 2015 (Yue & Zhu, 2021). The number of burglary cases reported per 100,000 people in various nations is shown in Table 1.1:

Table 1.1 Burglary Rate in Different Countries (“Burglary Rate,” 2020)

No	Country	Burglary in 2020	Burglary in 2019	Burglary in 2018	Burglary in 2017	Burglary in 2016	Burglary in 2015	Burglary in 2014	Burglary in 2013
1	New Zealand	1206.9	1429.1	1353.6	1465.2	1526.6	1324.2	N/A	1156.3
2	Sweden	803.4	751.8	781.4	908.4	905.4	922.3	916.2	888.5
3	Denmark	664.6	836.1	953.9	958.1	1,052.9	1,113.50	1,229.40	1,400.40
4	Chile	629.5	952.9	1086.5	1190.9	1,174.00	1195.9	1293.2	1,255.80
5	Austria	537.8	606.6	659.5	785.3	920.3	912	992.3	1,036.7
6	Australia	525.0	687.8	674.9	717.1	778.0	768.9	770.8	836.5
7	France	452.0	542.1	546.7	590.4	592.1	588.4	590.6	603.4
8	Belgium	407.9	562.6	610	657.2	695.3	812.9	859.3	895.9
9	Switzerland	379.2	423.9	455.9	489.0	555.4	633.6	776.3	847.6
10	Barbados	304.5	435.5	422.5	460.1	641.4	525.0	549.5	669.4
11	Greece	133.3	186.2	378.6	399.7	420.9	429.6	575.9	631.5

In comparison to other nations, Table 1.1 shows that New Zealand, Sweden, and Denmark had the most attempted residential burglaries in 2020. However, it is crucial to note that the actual number is higher than the supplied figures because many instances go unrecorded (van Dijk et al., 2007). In nations like Sweden, Denmark, Switzerland, and Austria, over 60% of burglary cases are recorded. In other nations, such as Hong Kong, Bulgaria, and Istanbul, however, such reporting rates are less than 40%. Disturbingly, in developing nations, recorded burglaries account for less than 20% of the total number of burglaries. de Oliveira (2018) upholds the statement that 62.07% of cases are not reported in Brazil and in the United States, only 13.1% of burglaries were reported to the police in 2016. As highlighted by van Dijk et al.

(2007), about half of all victims are dissatisfied with the police department's handling of their cases.

On a different note, this burglary has a financial, as well as physical, and emotional impact on the members of the household. In the United States, an average loss of USD 2361 per burglary is identified (Groff & Taniguchi, 2019). Kopp (2019) defends the statement that 7.9% of violence is reported along with burglary. According to Dinisman and Moroz (2017), 81% of burglary victims are emotionally affected with roughly 21% of all instances being highly affected. A victim might be an individual or a group of people who have been harmed or damaged as a result of this incident in a broad sense. Primary, secondary, and tertiary victims can all be classified as such (Stoliker, 2016). The primary victims suffer immediate loss and misery, whereas secondary victims also share the primary victim's suffering due to their close relationship. Both primary and secondary victims can be family members, and tertiary victims can be relatives, friends, or neighbors who hear about the incident (Stoliker, 2016).

In conclusion, residential burglary has obvious financial consequences and psychological costs, such as anguish, uncertainty, and dread of becoming a victim (Manning et al., 2022). This emotional or psychological harm due to burglary has an impact on the individual's family members, friends, and relatives. This also includes issues with adjusting to unfamiliar environments, which can lead to feelings of insecurity, causing individuals to recover more slowly (Dinisman & Moroz, 2017).

1.1.2 The Relationships Between Security Technologies and Burglary Crimes

Despite the increase in cases globally, burglary activity has dropped in several developed countries after the 1990s (Hodgkinson & Andresen, 2019). Countries such as the United States, Canada, Australia, and several European countries, for example, have seen a decline in cases (van Dijk et al., 2012). The decrease in cases may be attributable to the successful use of technologies in family security (Mawby, 2014). In a study by Tseloni et al. (2017a), burglary attempts are more than 7 times higher in less secure residences than in households with improved security measures. In addition, burglaries are 300% more frequent in residences without a security system, according to Kodali et al. (2019).

Several research studies that examine the effectiveness of various domestic security solutions also support the previous statement by Kodali et al. (2019). First, according to Hodgkinson and Andresen (2019), between 2003 and 2016, the number of home burglaries in Vancouver decrease from about 7000 to just less than 3000 cases. Second, burglaries in Belgium decline by 30% from 2005 to 2016 (Vandeviver & Steenbeek, 2019). Third, burglary attempts in the United States dropped by 27.4% and 37.1% in 2017 compared to 2013 and 2008, respectively, due to the use of technologies such as alarms and cameras in the home (Wolfe, 2018). Fourth, burglary rates in the Netherlands decrease by 26% each year as a result of built-in security measures in new homes. These security measures also contribute to a net 5% drop in total burglaries in the decade after the implementation (Tseloni et al., 2017b). Finally, as per 60% of the robbers, a security alarm forces them to look for a different and easier target. Furthermore, cameras and monitoring devices are identified as important deterrents in these cases (Blevins et al., 2012).

On the contrary, crime is higher in emerging countries than in developed countries, and there are considerable regional differences (Grote & Neubacher, 2016; Natarajan, 2016). Burglary rates have climbed in many developing countries in recent years (Kommey et al., 2018) such as India (Chitnis et al., 2016; Patil et al., 2019), China (Chen et al., 2017), Malaysia (Haslinda et al., 2020), and other countries. For this reason, scientists have identified a few factors that are contributing to the upsurge in these incidents. First, according to Tastan et al. (2019), burglary is a serious threat that has not been fully addressed particularly in low-income countries. Second, because crime statistics are more difficult to come by in developing countries, burglary research has mostly concentrated on developed nations (Ye et al., 2015; Chen et al., 2017). Third, according to Chitnis et al. (2016), inhabitants of third-world countries routinely neglect and underestimate the importance of home security. In India, for example, only 17% of people have a home security system (Patil et al., 2019). Similarly, while the use of preventative security measures is increasing in many developed countries, it is not growing at a similar rate in emerging countries (Tseloni et al., 2017a). In any case, Kommey et al. (2018) have concluded the discussion by arguing that the significant increase in the frequency of burglaries in developing countries has heightened the need for stronger home security measures.

In comparison, in poorer regions where people are less capable to afford security technologies, the number of burglary cases is higher (Hodgkinson & Andresen, 2019). Further, the largest influence on burglaries comes from living in an urban location (de Oliveira, 2018). Additionally, Chon (2017) has identified that homes in developing countries are far more vulnerable to residential burglary than houses in developed countries. This is due to the utilization of protective household measures in developed countries.

1.1.3 The Efficiency of Internet of Things-Based Security Devices

Security in homes has improved tremendously in recent decades and would continue to do so in the years ahead with equipment such as alarms, CCTV monitoring systems, door-window locks, and other security features. However, when the consumer is not present at home during an event of a crime, the buzzer or alarm becomes useless. As a result, even after these security measures have been put in place, the residence remains unsafe (Anitha, 2017). Apart from that, CCTV systems have a number of significant flaws. Firstly, these devices do not provide real-time event information. Secondly, because this is an analog system, it continues to record events even when no disruption occurs. Finally, the continuous storing of events and video streaming necessitates a large amount of bandwidth support and storage (Surantha & Wicaksono, 2018). Most importantly, according to de Oliveira (2018), none of these devices can effectively protect homes against burglary.

IoT-enabled security solutions can, in reality, overcome these drawbacks. As an example, IoT employs a variety of sensors, such as motion sensors, vibration sensors, and door open detection sensors, to monitor household activities from afar (remotely). Furthermore, using a real-time notification system, the IoT system can notify the user of any questionable events. Traditional alarm systems, for example, are designed to make a loud noise in order to alert those in the vicinity of an intruder. As technology advances, IoT systems are designed to send a signal to a central monitoring station, informing of the location of the alarm and also alerting the police. Therefore, it can be claimed that an IoT-enabled security system provides considerably superior security to a standard home security system (Surantha & Wicaksono, 2018; Ijaz et al., 2016).

1.1.4 The Acceptance of Internet of Things-Based Security Devices

IoT-enabled security devices are popular in different nations. First, 'KRC Research', a research unit of Interpublic Group, has conducted quantitative research in four countries such as the United Kingdom, Germany, Japan, and the United States where 23% of respondents have already implemented an IoT-enabled security system. In addition, 80% of the respondents have planned to implement this system in the next few years ("GSMA: The Internet of Things," 2015). Second, in the United States, the primary motivation for adopting a smart home is home security. Smart cameras (40%) are the most popular security gadgets, followed by video doorbells (26%) and smart locks (13%) (Meola, 2016). Third, machine-to-machine (M2M) services are an essential example of the IoT, and they assist to accelerate the expansion of IoT devices. Home security applications are also predicted to account for 48% of all M2M connections by 2022 ("5G: Future of IoT," 2019). Fourth, the rate of crime in South Korea grows by 37% between 2002 and 2011. As a result, the national police agency begin to use IoT to detect and reduce these crimes (Byun et al., 2014). Fifth, in 2016, Gartner performed an online poll with approximately 10,000 respondents from the United Kingdom, the United States, and Australia to determine the adoption of various IoT-based home automation products. According to this survey, the majority of people use smart alarms to keep their homes safe (Forni & Meulen, 2017). Sixth, smart video doorbells reduced burglary by 55% in 2015 through a pilot program maintained by the Los Angeles police department (Harris, 2018). Finally, in 2017, over 35% more people installed high-tech security systems in their homes, such as sensors and cameras which could alert Dubai police to any unwelcome events. As a result, the rate of burglary in Dubai drops by 20% (Ramahi, 2018).

On the flip side, according to Shenkoya (2020), IoT implementation in developing nations is still in its infancy and has yet to gain widespread acceptance. Mital et al. (2018) and Almagari et al. (2020) support this statement, claiming that IoT adoption in these nations is still restricted. Several IoT adoption roadblocks have been identified which is important to note (Hopah & Vayvay, 2018; Miazzi et al., 2016, Ndubuaku & Okerefor, 2015). Low internet access, however, is a key barrier for underdeveloped countries in terms of allowing IoT, according to Miazzi et al. (2016). The IoT, indeed, demands a persistent internet connection across all devices. Internet penetration rates in developed, emerging, and least developed countries, on the other hand, are estimated to be around 90%, 57%, and 27%, respectively ("Measuring digital development: Facts and numbers," 2021). In addition, the lack of an infrastructure policy on IoT adoption must also be filled (Shenkoya, 2020). For this reason, IoT adoption for home security in poorer nations is unlikely to be widespread.

Surprisingly, individuals in developing countries are also interested in using IoT devices to keep their homes safe from burglaries. To illustrate, a survey from a total of 78 participants in Pune, India, find that 95% of respondents favor better security measures that can be implemented by utilizing various IoT security technologies (Chitnis et al., 2016). This positive sentiment is also identified among citizens of Indonesia who find IoT security gadgets to be quite helpful in maintaining the security of their houses (Yasirandi et al., 2020).

1.1.5 Burglary Cases in Dhaka City

Dhaka ranks 313 out of 338 cities in the ranking of overall security with a safety index point of 32.75 which ensures that Dhaka is one of the least safe cities in

the world (Papadopoulos, 2019). On the flip side, a popular database, Numbeo, presents relevant information to support the assertion that crime rates in Dhaka city have not significantly changed in recent years ("Crime Index by City," 2019). Similarly, the Economist polled residents of 60 cities between 2017 and 2019 about a range of security-related issues. In terms of overall rankings, Dhaka city came in at position 58 in 2017 and 56 in 2019 ("The Economist intelligence unit," 2017; "The Economist intelligence unit," 2019) which confirms that crime is one of the major concerns for Dhaka city. As previously highlighted, domestic burglaries are one of the most common crimes worldwide, and this is true in Bangladesh as well (Khatun & Islam, 2018). The statistics on existing criminal activities in Dhaka city are presented in Table 1.2 which is based on information from the Bangladesh police department.

Table 1.2 Crime Statistics of Dhaka City

Year	Number of Robbery Cases	Number of Murder Cases	Number of Kidnapping Cases	Number of Theft Cases	Number of Burglary Cases	Source
2010	220	245	139	1915	555	("Crime Statistics," 2010)
2011	294	259	118	2050	589	("Crime Statistics," 2011)
2012	222	264	149	2240	592	("Crime Statistics," 2012)
2013	241	270	165	2196	534	("Crime Statistics," 2013)
2014	265	262	176	2130	650	("Crime Statistics," 2014)
2015	205	239	146	1711	642	("Crime Statistics," 2015)
2016	131	165	103	1516	547	("Crime Statistics," 2016)
2017	103	218	85	1197	554	("Crime Statistics," 2017)
2018	83	216	75	1290	613	("Crime Statistics," 2018)
2019	10	19	9	127	49	("Crime Statistics," 2019)

It is important to note that there has been no discernible improvement in preventing criminal activity, particularly burglary attempts. However, during the Covid-19 pandemic, only 137 cases are documented countrywide (Sakib & Shohag, 2022). Furthermore, many illegal activities go unreported (Islam et al., 2018; Khan,

2015). As a result, the publicly available data do not reveal the true number of incidents which could be far greater than the reported scenario (Chowdhury, 2014; Islam et al., 2018).

1.2 The Motivation Behind the Research

The internet penetration rate in Bangladesh is 73.06% (“Teledensity & Internet Penetration”, 2021). Earlier, Bangladesh set a goal of having 100% internet connection by 2021 (Chakraborty et al., 2020). The total number of internet subscribers reached 126.60 million in November 2021 (“Internet Subscribers”, 2021). Alongside this, Dhaka city has better internet facilities than the other cities in the country (Chandrima et al., 2020). Fortunately, the government of Bangladesh legalized the import of IoT products in April 2018 through IoT import policies (“Guidelines to import IoT devices in Bangladesh,” 2018). Consequently, IoT-aided security products are now available in the local market (Ayon, 2019; Moretaza, 2018; “The year of 5G,” 2019). In addition, Bangladesh is one of the narrowband IoT (NB-IoT) empowered nations worldwide (Mahbub, 2020). In particular, NB-IoT is a licensed low-power wide-area network (LPWAN) technology based on the current long-term evolution (LTE) standard and capabilities (Li et al., 2018). Notably, the adoption of IoT depends on the networks it operates, and NB-IoT can ensure the quick deployment of IoT applications in Bangladesh (Mahbub, 2020; Feurer 2018). Essentially, the utilization of IoT is relatively new in Bangladesh, but its popularity has been rising among researchers, consumers, and organizations (Sultan, 2017). Therefore, it can be assumed that Dhaka city has the necessary support and resources to implement IoT devices in homes for home security.

From a different viewpoint, according to the census 2022 conducted by the planning ministry of the Bangladesh government, the total population in Dhaka metropolitan city is 10.2 million (“Population and Housing Census”, 2022). Additionally, people from different regions of the country are constantly trying to get settled in Dhaka city. Therefore, it can be assumed that Dhaka's population represents the general population of Bangladesh (Khan et al., 2014). Based on the crime statistics shown in Table 1.2, it can be said that burglary is one of the most common crimes, and most houses in Dhaka are not safe. Due to these illegal activities, inhabitants of Dhaka city are not satisfied with their home safety (Khan, 2015).

Nonetheless, an IoT-enabled security system can be a useful tool for preventing and reducing burglary attempts (Abu et al., 2018; Jena et al., 2019). Therefore, it is anticipated that burglary and other criminal attempts at households can be reduced if an IoT-empowered security system can thoroughly be introduced to the household of Dhaka city. Furthermore, this research can also benefit other cities with similar economic conditions and social customs where burglary is an issue.

1.3 Problem Statement

According to Macik (2017), the global research interest in IoT-related topics began around 2008. However, since 2013, several high-quality journals indexed in Scopus, Web of Science, and other databases have observed a considerable rise. Almost all of the publications are about IoT's technical development in computer and electrical engineering. A small amount of research related to this research (around 8.6%) is in management, social science, and others (Macik, 2017). This includes papers on consumer adoption of IoT in various nations (Luthra et al., 2018; Miazzi et al., 2016). In addition, some research on smart homes and home automation has also

been carried out (Yang et al., 2018; Park et al., 2017; Baudier et al., 2020). Furthermore, academics have focused on user adoption of IoT devices and services (Hsu & Lin, 2016; Hsu & Lin, 2018). It is important to note that household security issues are partially included as one of the elements or constructs in these papers (Hsu & Lin, 2016; Hsu & Lin, 2018; Yang et al., 2018; Luthra, et al., 2018; Miazi et al., 2016). Nonetheless, quantitative-based empirical research on consumer acceptance of IoT-enabled security facilities in homes is currently scarce and underexplored.

IoT adoption, on the other hand, is vital to make users' lives easier (Seliem et al., 2018; Liu et al., 2019; Abdullah et al., 2018; Saleem et al., 2018, Zandrato et al., 2019). Currently, only developed countries have seen such widespread adoption of IoT, which includes higher acceptability for home security. However, in developing nations, this acceptance is relatively low. Despite being a developing country, Bangladesh has several benefits regarding IoT adoption, as illustrated in section 1.2. Likewise, the Bangladesh government has recently developed a 'National IoT Strategy' to address residents' economic, social, environmental, and global needs. Additionally, Bangladesh has implemented a few policies to encourage IoT use where security issues are incorporated for end-users ("National Internet of Things Strategy," 2020). Despite all the benefits, however, IoT adoption in Bangladesh is rather low (Parvez et al., 2021). It is worth mentioning that the purpose of this research is to enhance consumer adoption of IoT-enabled security devices to reduce burglary crimes. IoT is primarily employed for business-to-business (B2B) applications in Bangladesh (Parvez et al., 2021), and unfortunately, consumer engagement has been disregarded. As a result, understanding consumer approval and determining the factors impacting user adoption of IoT from the perspective of household security among Dhaka inhabitants is crucial to improving adoption. This viewpoint is also shared by

Karahoca et al. (2018) and Gao and Bai (2014), who both advocate for more significant research into the factors that influence the consumer acceptability of IoT devices.

Burglary is one of the significant security issues in Dhaka city, as stated previously; several factors are capable of defining the intensity of the threat, such as severity and vulnerability. On the other hand, self-efficacy, response efficacy, and response cost outline the procedure to defend against the threat positively (Al-ghaith, 2016; Verkoeyen & Nepal, 2019). Moreover, attitude and social influence are vital for individual adoption of any technology like IoT (Karahoca et al., 2018; George et al., 2021; Gao & Bai, 2014; Al-Momani et al., 2018). Therefore, these factors are required to evaluate the intention to adopt the IoT-enabled security system in Dhaka households. Furthermore, personal innovativeness and perceived trust should be considered moderating variables because these are crucial in adopting any new technology (Cheng, 2014; Thakur et al., 2016; Xin et al., 2015; Mackert et al., 2016; AlHogail, 2018). According to Pal et al. (2019) and Sung and Jo (2018), a more innovative person has a better attitude about using new technology such as IoT which may contribute to increased user adoption. Furthermore, a higher level of trust increases the possibility of new technology adoption (AlHogail, 2018; Pal et al., 2019).

In short, it is vital to determine the factors that influence the intention to adopt IoT for home security at the households in Dhaka city. Moreover, incorporating personal innovativeness and perceived trust as moderating variables should significantly impact users' adoption intentions.

1.4 Research Questions

1. What are the factors that influence the intention to adopt IoT for home security at the households in Dhaka city?
2. How does personal innovativeness moderate the relationships between influencing factors and the intention to adopt IoT for home security at the households in Dhaka city?
3. How does perceived trust moderate the relationships between influencing factors and the intention to adopt IoT for home security at the households in Dhaka city?

1.5 Research Objectives

1. To determine the factors that influence the intention to adopt IoT for home security at the households in Dhaka city.
2. To study the moderating effect of personal innovativeness on the relationships between influencing factors and the intention to adopt IoT for home security at the households in Dhaka city.
3. To study the moderating effect of perceived trust on the relationships between influencing factors and the intention to adopt IoT for home security at the households in Dhaka city.

1.6 Significance of the Research

The Bangladesh government has proposed several measures to increase IoT usage. The need to invent, incubate, and finance IoT technologies for security objectives has also been highlighted. Nonetheless, these techniques have mostly prioritized business communications in the IoT sector, while consumer behavior has been overlooked. On the other hand, the intention of consumers to use IoT is assessed

in this research, along with influencing factors and moderators. As a result, this research can help to enhance IoT usage and provide new insights to present policies. Furthermore, this research can raise knowledge and acceptability of IoT devices which can aid in achieving two additional benefits. Firstly, burglary can be minimized, and Dhaka's overall law and order situation can be improved. Secondly, these devices have the potential to make homes more secure than before which may increase the level of ease. Furthermore, individuals may feel less concerned when they remain outside and their homes are left unattended.

Notably, the research model incorporates two separate theories, protection motivation theory (PMT) and attitude-social influence-self-efficacy (ASE), as well as two moderators, personal innovativeness and perceived trust. This research stands out as one of the first to include all of these theories and moderators in a single research model. As a result, this research can enhance conceptual knowledge and comprehension of IoT adoption for home security by studying user adoption using the proposed model. The findings of this research have important implications for companies and entrepreneurs trying to develop IoT marketing and investment strategies. Furthermore, customer adoption is expected to rise if these characteristics are included in company activities. Importantly, this proposed model is likely to serve as a catalyst for future research into the factors that drive individual IoT adoption for security considerations.

1.7 Definition of Key Terms

Table 1.3 Definition of Key Terms

No	Terms	Definition	Source
1	Perceived severity	It is specified as the extent of the severity of any harm that a person perceives.	Janmaimool (2017)
2	Perceived vulnerability	It is specified as the understanding of the individual's vulnerability to harm.	
3	Perceived self-efficacy	It is specified as the understanding of an individual's capacity to execute the behaviors.	
4	Perceived response efficacy	It is specified as the perceived efficiency of suggested risk reduction behaviors.	
5	Response cost	It is specified as the expense and effort of carrying out the required behavior.	
6	Protection motivation	It is defined as the intention to execute the desired behavior.	Murtagh et al. (2019)
7	Attitude	It is defined as the expectations or current observations of the behavioral benefits and drawbacks.	Rodríguez-Calvillo et al. (2011)
8	Social influence	It is defined as the extent to which a person is motivated by others' beliefs.	
9	Personal innovativeness	It is defined as the extent to which a person accepts new ideas compared to others.	Agarwal and Prasad (1998)
10	Perceived trust	It is defined as an individual's reliance on another party under conditions of dependence and risk.	Currall and Judge (1995)
11	Intention	It is specified as the degree to which an individual has devised a deliberate plan to conduct or not to perform some specified potential behaviors.	Amelia and Ronald (2017)

1.8 Outlines of the Thesis Chapters

This dissertation is organized into six chapters. First, background information is supplied in chapter 1, which leads to problem statements, research questions, and objectives. Subsequently, chapter 2 looks at the current literature on adoption ideas. Furthermore, an acceptable model is chosen, together with argumentation for the relevance to the research's environment. In addition, a list of hypotheses is proposed following the research model. Afterward, chapter 3 provides a thorough explanation of the methods that are used. Following that, based on the data received from the final survey, chapter 4 examines the consumer's responses. Chapter 5 goes through the results of the research questions as well as the hypotheses that follow them. Finally, in chapter 6, the achievement of the objectives, research contributions, and limitations with directions for future research are explored.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The primary goal of this chapter is to examine the current state of information on IoT adoption among consumers from various domains. Following that, the theories and models, that have been used to forecast, explain and comprehend people's adoption and usage of IoT technology, are examined. Hence, this chapter is divided into nine sections to meet the information demands of a broad range of readers. To begin with, the current status of information and communication technology in Bangladesh is briefly illustrated in the second section. In the third section, the basic concepts of IoT are briefly explained. In the fourth section, essential information on IoT-based security devices such as present growth, market value, and some example devices are concisely elaborated. In the fifth section, the basic concepts of different adoption theories, their application to IoT-related studies, and the limitations of these theories are discussed. Afterward, a suitable model is proposed in the sixth section. Following the research model, the hypotheses are proposed in the seventh section. Subsequently, the reasons for choosing moderators and the description of the moderating variables are discussed in the eighth section. This section also follows the proposal of some more hypotheses, and the chapter summary is provided at the end.

2.2 Status of Information and Communication Technology in Bangladesh

One of Bangladesh's most important and quickly expanding areas is information and communication technology (ICT) (Dey et al., 2019). The government has designated it as a 'thrust sector', and a variety of measures have been developed to support it (Hoque, 2020; Aziz, 2020). According to Shamim (2022) and Islam et al.

(2021), significant progress has already been achieved in the ICT industry over several years toward creating a Digital Bangladesh (vision 2021), and more measures are being planned to create a Smart Bangladesh (vision 2041). Besides, Bangladesh is aiming toward vision 2041 and DELTA plan 2100 after completing vision 2021's goals (Usman et al., 2021). On the other side, Bangladesh's economy has grown strongly over the previous ten years, growing by 8.2% in the fiscal year 2019—the fastest rate in the Asia-Pacific region, where ICT accounts for 29.2% of GDP (Husain & Kamruzzaman, 2020; Ahmed, 2022; Islam & Inan, 2021).

Furthermore, Bangladesh is now seen as an emerging nation due to its quick growth in the usage of mobile phones, accessibility to internet connections, ICT export revenue, and extensive use of ICT in a variety of governmental operations (Azim, 2022). Bangladesh's ICT market reached USD 1 billion in 2018. By successfully launching the nation's first satellite in 2018 to improve mobile and internet service, Bangladesh enters the space race. Moreover, 4G mobile services have been available throughout the nation since 2018 while 5G is scheduled to start in 2024 (Nourani et al., 2020). Furthermore, Bangladesh's ICT sector has made it one of the most obvious targets for international organizations for a number of years (Rumi et al., 2020). The activities and services of several top ICT businesses, including Apple, Samsung, HTC, Nokia, IBM, Google, and Facebook, have begun. In addition, young entrepreneurs in Bangladesh are simultaneously urged to take up technology enterprises. Both of these initiatives result in a significant increase in employment; assist Bangladesh in quickly achieving upper middle-income status (Ahmed, 2022; Rumi et al., 2020)

Moreover, the Internet of Things (IoT) represents a new paradigm shift in ICT with enormous potential for day-to-day activities (Sultana & Tamanna, 2021). Bangladesh has launched numerous new IoT applications in several spheres, some of which are listed below, in order to realize vision 2041 with the necessary advancement in the socio-economic aspects. The government of Bangladesh has provided funding to establish a cutting-edge IoT lab to create and train IoT experts, DataSoft along with Japan have begun creating 10,000 smart houses, a smart car monitoring system has been released by Grameen Phone and to give manufacturers real-time visibility and assure high-quality goods, Robi launched "nFactory" (Parvez et al., 2021). As a result, these innovative IoT applications can assist to gain better socio-economic conditions for the citizens (Chakraborty et al., 2020; Parvez et al., 2021).

2.3 Definition of the Internet of Things

In 1991, Mark Weiser first predicted the idea of pervasive computing and Kevin Ashton first proposed the internet of things (IoT) as a communication medium through radio-frequency identification (RFID) tags in 1999. At this moment, IoT is inspired by these two ideas to connect and create communication between every living and dead object (Chin et al., 2019). For the last two decades, IoT has become versatile and observed to use in different sectors. Therefore, this IoT cannot be properly defined since no standard definition has been established yet (Sidek & Ali, 2019).

IEEE defines IoT, in a broad sense, which is a collection of devices that are linked to the internet and integrated with sensors (Minerva et al., 2015). Abdur et al. (2017) further argue that IoT assists numerous amounts of computers, individuals, and utilities to communicate and exchange data with each other. However, in many research papers, the following two definitions of IoT have been highly used and

related to this research. Formerly, according to the cluster of European research projects, ‘things’ of IoT are considered as the dynamic participants in the industry, knowledge, and social systems in which they can engage and connect. These devices share data with the surroundings when autonomously responding to and shaping physical world activities by operating processes that can act with or without human interference (Gubbi et al., 2013). Eventually, the international telecommunication union (ITU) states that IoT is a digital network for the information association that allows progressive services through communicating with virtual and real entities based on current information and communication technologies (Saint & Garba, 2016).

Based on these above two definitions, the IoT can be elaborated in the following way. A world can be visualized where more than billions of entities can sense, read, interact, and share relevant information through internet protocol (IP) networks. Such integrated structures include data collection, processing, regular intervention, management, and decision-making information (Gupta & Gupta, 2016). These are all possible due to the establishment of IoT which is not referring to a particular technology, but a combination of different hardware and software innovations (Patel et al., 2016). It aims to connect ‘things’ anywhere, with anyone at any time. This ‘thing’, in IoT, can be considered an entity; it is either a communication device or a dumb non-communicating object. Thus, everything can participate and communicate over the internet from an intelligent device to a tree leaf or a bottle of water (Aazam et al., 2015).

Specifically, this research aims to measure the consumer adoption of IoT-enabled security devices. Therefore, the growth and market share of IoT-enabled security devices is analyzed in the subsequent section.

2.4 Existing Literature on Internet of Things-Based Security Devices

As reported by D'mello (2019), the market value of IoT-empowered security products was USD 300 million, and USD 400 million in 2014, and 2019, respectively. In contrast, the value is expected to increase to USD 1.4 billion in 2029 with a compound annual growth rate (CAGR) of 12% from 2019-2029. On the contrary, the market value is claimed to be USD 618.83 million and 3.2 billion in 2017 and 2026, respectively, with a CAGR of 20.1% (“Research and Markets,” 2019). An ambitious CAGR is acquired to be 27% (Kline, 2017) which led the market value to USD 15.6 billion in 2021. Furthermore, the lowest CAGR is learned to be 10.4% during the period 2018-2023 (“Home Security System Market,” 2018). This research also claims that the market value was USD 40.66 billion and USD 45.58 billion in 2017 and 2018, respectively, and it is predicted to upsurge to USD 74.75 billion in 2023. In addition, several smart home products like lighting, entertainment, energy management, HVAC controller, and security are analyzed for the period 2012-2020 (million in USD) in the Asia Pacific region (“Industry Insights,” 2014). To a large extent, these security devices are detected to be one of the most significant products in the smart home market (see Figure 2.1).

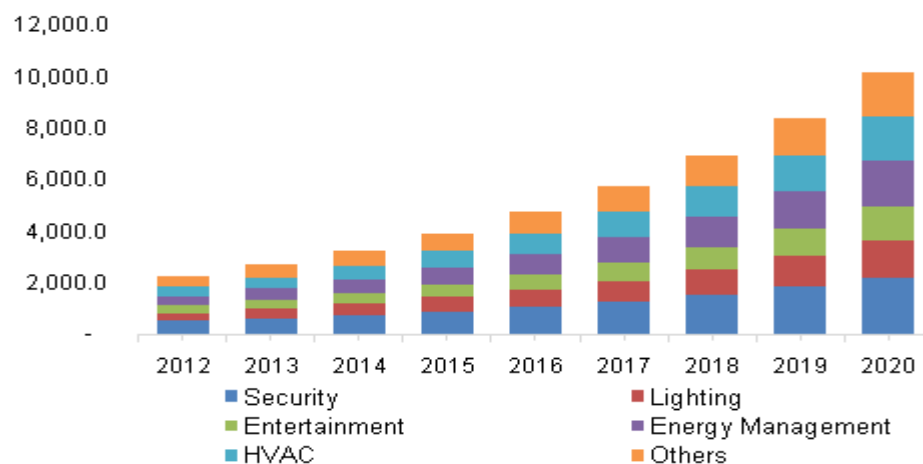


Figure 2.1 Smart Home Products Market in the Asia Pacific Region (“Industry Insights,” 2014)

Subsequently, the market of smart home appliances rose 31% in 2018 with USD 643.9 million shipments and is expected to grow by USD 1.3 billion in 2022 with an annual growth of 30.8% (“Security: Smart Home Devices Market,” 2018). In particular, security devices like IP cameras, window-sensor, and door locks are predicted to achieve a growth rate of 27.3%. Thus, it is predicted that these security products would be the second most consumed products by 2022 after entertainment products (see Table 2.1).

Table 2.1 Shipments and Market Share of Smart Home Devices (“Security: Smart Home Devices Market,” 2018)

No	Product Category	2018 Shipments (in millions)	2018 Market Share	2022 Shipments (in millions)	2022 Market Share
01	Home Monitoring/Security	97.7	15.2%	244.9	19.4%
02	Lighting	37.7	5.9%	104.6	8.3%
03	Smart Speaker	99.8	15.5%	230.5	18.2%
04	Thermostat	13.6	2.1%	37.5	2.9%
05	Video Entertainment	310.5	48.2%	457.5	36.2%
06	Others	84.5	13.1%	189.3	15.0%
	Total	643.9	100.0%	1264.3	100%

Finally, the consumption of these IoT home security devices is seen to diverge in different regions too (“Connected Home Security Market,” 2019) (see Figure 2.2). Among the regions, North American and East Asian people are the prime consumers of these products where a comparatively low acceptance is detected in the Middle East, Oceania, Latin America, and Africa. Most markedly, a high adoption is also predicted in South Asia where Bangladesh belongs. Therefore, a high-potential market in South Asia can create numerous business opportunities for IoT-supported security products (“Connected Home Security Market,” 2019).

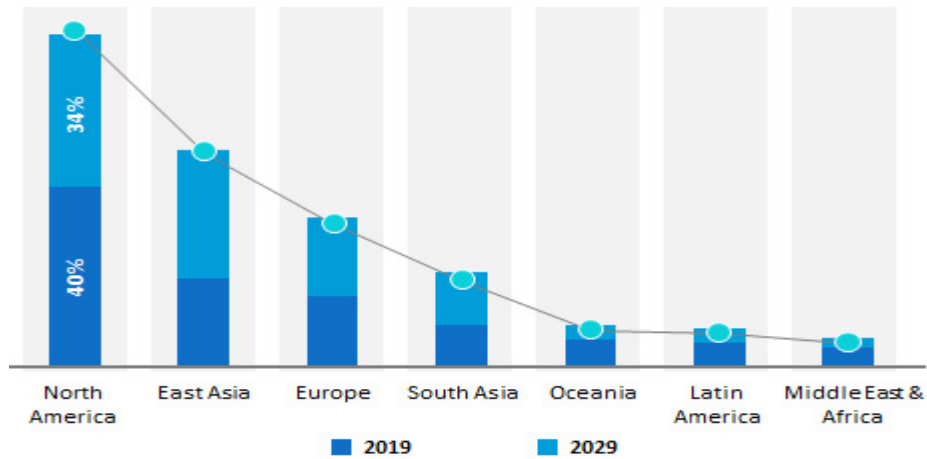


Figure 2.2 Market of Home Security Devices by Region (“Connected Home Security Market,” 2019).

Hence, it is clear from the above discussion that these home security products have a high contribution to increasing the popularity of IoT technology. Additionally, though these achieved CAGR and market values are not consistent in different research works, the importance of these products cannot be ignored. Most significantly, high annual growth is noticed, confirming the rising market value and availability of these IoT-assisted security products. Nevertheless, the most common devices are the following four types of IoT security devices such as cameras, alarms, locks, and detectors (“Connected Home Security System Market,” 2017).

In contrast to basic security cameras that store data in a household computer or client systems, these IP cameras can support both the real-time monitoring system and cloud storage. Most impressively, these cameras can identify unauthorized objects and notify the owner immediately about their presence through instant messages (Pino, 2020). Although these cameras are less expensive than analog ones, their structural similarities lead to the system's selection (Kovář et al., 2016). Dissimilar to the regular alarm system, these IoT alarms can be set independently or integrated with other security devices. Besides, this smart system uses wireless technology within a home

network and has the opportunity to be operated through smartphones (“What Is a Smart Alarm System,” 2020). It is anticipated that sales of these smart alarm systems reached USD 4.63 billion globally by 2021 with a growth rate of 19.37%. The usage of these devices in the United States increased by 15–20% after 2010 (“Connected Home Security System Market,” 2017). Further, users, at present, prefer these smart locking systems as an alternative to mechanical locks, and their growth rate is followed to be stable in recent years (“Connected Home Security System Market,” 2017). These smart locks can supplement or replace the regular door lock or deadbolt because these devices can lock-unlock the windows and doors without using any key or remotely. Additionally, these gadgets can assist in deciding whether to let or reject somebody enter or leave the property while the system owner is not around (Wolpin, 2019). Finally, the smart detection system includes the detection of fire-carbon monoxide along with the heat-ventilation-air condition (HVAC) system and can provide real-time notification to smartphones which the old system cannot do (“Connected Home Security System Market,” 2017). These HVAC systems can integrate data mining techniques for fault finding and analysis. The system also incorporates cloud computing and artificial intelligence systems for improved performance (Dey et al., 2020, Javed et al., 2017).

The market share and growth rate of these devices are demonstrated in Table 2.2. The data confirm significant macroeconomic improvement and forecast smart devices that are anticipated to propel the worldwide home security market's expansion. The most popular smart gadgets in 2016 were smart alarms, IP cameras, smart locks, and HVAC systems. Nonetheless, a substantial growth rate is seen for every item, indicating that people value all of these gadgets almost equally. The