DATA PRIVACY ISSUES IN INTERNET OF THINGS (IOT) FOR SMART HOMES: A CASE STUDY OF NEPAL

Sandesh Gurung[1] and Dolma Kumari Sherpa[2]
[1] PG Scholar, Lord Buddha Education Foundation, Kathmandu, Nepal
[2]Programme Leader (IT), Lord Buddha Education Foundation, Kathmandu, Nepal

ABSTRACT

IoT is one of the emerging technologies today having its impacts on our daily lives. IoT has influence over various domain from a simple wearable device to the huge industrial uses. Smart Home is one of the most talked about IoT domains which has already affected large population along with its chances of increase to more than we believe. The technology has become an essential milestone in smart home environment to bring convenience and efficiency in our daily doings. Also, the technology has become an increasingly popular topic for researchers. Despite its popularity and highly usage, the concern of data privacy issues is important to better understand the privacy implications in smart home usage. Connection of smart home devices to the internet and sharing data and information in between results in new security challenges and problems. Thus, using the technology without prior knowledge and preparedness could result to different security attacks and risks for smart home users. While in the context of Nepal, the smart home technology is not a new concept but has less impact on residents. The population in Nepal seemed to be less or not aware of smart home technology and its data privacy issue considerations. The following research provides the background information about IoT and smart homes along with its challenges in data privacy perspectives and provide meaningful recommendations in the context of data privacy vulnerabilities in smart home environment. In addition, the research also examines the understanding and awareness of IoT and smart homes among the population in Nepal through survey procedure. The recommendations and suggestions to encounter the possible threats and attacks in smart home environment after the careful data analysis adds useful contribution for smart home consumers as well as the suppliers/suppliers.

Keywords: Internet of Things, Smart Homes, Data Privacy Issues, Data Security

1. Introduction

1.1 Introduction

Smart home is one of the most talked and essential domains of Internet of Things (IoT) applications. Smart home consists of connected smart devices with sensors, RFIDs, actuators, laptops, smart phones, PDAs, and other smart home appliances to share the network resources and information within connected things being in the internet connection. The technology has been used in various beneficial systems and in smart homes as energy management, automation, security purposes, and to ease the daily doing activities (M. Bala Krishna, 2016). The concept smart home existed for many years but has become the topic of attention for researchers in recent times in higher pace (Shafiq Ul Rehman, 2016). Securing the smart home system is challenging due to its heterogeneous and complex nature which consists of various devices with different mechanisms (Shafiq Ul Rehman, 2016). At the same time, due to its nature of connection and controlling mechanism through remote access, the system is more prone to remote controls and attacks. The following research is based on the case study of Nepal, presents the current status and practice of smart home usage, user awareness on smart homes including knowledge about IoT and smart homes, their comfortability of usage, awareness on smart home security threats,

awareness on data privacy issues caused in smart home ecosystem, awareness on consequences of smart home threats and attacks, knowledge on data privacy preservation techniques or their approach towards handling the threats and attacks. From the survey conducted on the research domain, the following research identify smart home practice and awareness status among smart homes users in Nepal along with the analysis and evaluation on data privacy threats and attacks, their consequences and security requirements.

1.2 Background

From the time when people used to communicate through symbols, pictures and complex communication languages to this time of modern and advanced technologies, the evolution of the technologies is emerging rapidly. The modern technologies such as machine learning, cloud computing, edge computing, artificial intelligence, virtualization, Internet of Things (IoT) are most talked about and evolving technologies today. Internet of Things (IoT) is one of the attention-grabbing technologies that are widely used in various sectors such as health care, insurance, business, transports, logistics, banking, home appliances etc. The technology has greater impact on today's community as well as in personal usage with wider coverage ranging from wrist band, home appliances, cities, affecting our everyday activities. It is estimated that between 25 billion and 50 billion devices will be IoT enabled device by 2020 and 97.5% of the global population will be connected with IoT devices by 2050 (Seaman, 2015).

1.3 Smart Homes in Nepal

Nepal has a great success in the digital journey with mobile penetration exceeding 100%, internet penetration reaching 60%, and 2.25 million new internet users in 2017 alone according to Nepal Telecom Authority (Technology, 2018). With such rapid growth of internet and modern technologies, smart home system is one of the fairly a new concept which is being implemented in high-end residences, large offices, and recently increasing in medium-sized households as well. Besides that, majority of smart home users in Nepal are less aware of the consequences that may occur from threats and attacks on smart home environment they exist. In addition, they are also less knowledgeable on the security and preventive measures on threats and attacks in smart home environment.

There are few smart homes service providers serving the nation to drive toward automated homes. GA Builders (P.) Ltd. is a construction, consulting, engineering company which has implemented smart homes projects in their project list providing the services such as smart lightening, temperature, security, smart windows and doors, multi-media etc for smart home ecosystem (LTD, 2018). Likewise, Home Automation Nepal is providing its services in various sectors such as hotels, restaurants, educational institutions, hospitals with automation services in areas such as security, lightening, surveillance, music, climate, digital door locks, visitor management, central vacuum system etc (Nepal, 2019).

1.4 Problem Statement

Usage of IoT devices is increasing in home appliances with the trend of latest and advanced technology evolution. At the same time, awareness of how secure are those devices to use in our daily doings is a serious concern. Due to the heterogeneous nature of the technology (IoT), smart home environment could be more vulnerable from intruders. When connecting to a home through internet access, intruders can bring various threats and attacks and control the home from anywhere in the world compromising the smart home users' privacy. The data and information we provide to function those devices, are those personal data safe or not? Are those data being accessed by third parties? Are those data secure from outsiders (attackers)? The data privacy issues arising in the field (smart homes) and their adequate solution is a serious concern. At the same time, the country like Nepal adopting IoT and

smart home systems as a new concept need to be aware of the data privacy issues and their preservation techniques in smart home environment.

The current issues or problems in smart homes in the case of Nepal are:

- Lack of awareness on IoT and smart homes
- Lack of awareness on data privacy issues in smart homes
- Lack of preparedness on data privacy issues in smart homes

1.5 Research Questions

From the literature on the proposed topic of research, it is found that more research is necessary on data privacy issues in smart home environment. Based on the case study of Nepal, no academic research relating the data privacy issues was found which has been identified as the major gap of the research topic. In addition, the important research on advantages, drawbacks and security countermeasures are also not done on smart home environment. Thus, for the research on identified gap from literature, following research questions has been prepared.

1. What are the advantages and drawbacks of IoT technology usage in smart homes?
2. What are the data privacy and security challenges facing by IoT technology implementation in smart homes?
3. What are the possible recommendations, suggested security measures and protection steps for securing personal data and information in usage of IoT devices in smart homes?

1.6 Research Aims and Objectives

1.6.1 Aim of the research

The main aim of this research is to analyze, evaluate and explore effective recommendations on personal data privacy issues arising in IoT enable devices in home appliances.

1.6.2 Objectives of the research

1. To explore the IoT technology working mechanisms and framework in smart homes along with their advantages and drawbacks of usage.
2. To explore data privacy and security challenges facing by IoT implementation in smart homes.
3. To recommend and suggest the security measures and protection steps for securing personal data and information in usage of IoT devices in smart homes.

1.7 Significance of the Study

The research work believes to serve the community with privacy awareness and safe guarding recommendations from being vulnerable who are using IoT enabled devices in their daily activities precisely in smart homes. The research work also believes to solve the existing problems facing by IoT technology consumers. The research work will conduct online as well as offline survey as well as the primary and secondary data collection through various sources to deliver the fruitful contribution to data privacy issues in smart home ecosystem. As the research is based on the case study of Nepal along with the broad study to worldwide coverage, the valuable contribution and deliberation of the research will be much beneficial for Nepali smart homes users.

1.8 Limitations and Scope of the Study

The following research evaluates the data privacy issues in IoT enabled smart home environment from the data and information collected through different sources and gives the adequate countermeasures to overcome the problems identified. Although the final findings and outcomes of the research intends

to cover the overall community of IoT enabled smart homes, it is best suited to the case of Nepal as the research is based on case study of Nepal.

1.9 Research Hypothesis

Research hypothesis are testable statements that has link with research questions. In other words, research hypothesis bridges the gap to research questions based on the variables to be measured/tested. In general, null hypothesis says that there is no association between testing variables while alternate hypothesis says that there is association between testing variables (Statistics Solutions, 2019). Based on the research objectives and research questions, the following research aims to test some variables' association those are linked to research questions. As the research adopts quantitative approach along with qualitative approach, the hypothesis is tested for quality output based on the survey. The hypothesis constructed based on connection to research questions and their relating variables are given below.

Table 1: Research Hypotheses

Hypothesis	Statement	Data Analysis Type
H_1	A population in Nepal who understand IoT technology are not aware of advantages and drawbacks of smart homes usage.	Crosstabulation (Chi-Square Test)
H_2	A population in Nepal who understand smart home systems are not aware of advantages and drawbacks of smart homes usage.	Crosstabulation (Chi-Square Test)
H_3	A population in Nepal who understand IoT technology are not aware of data privacy issues for smart homes.	Independence Sample T-Test
H_4	A population in Nepal who understand smart home systems are not aware of data privacy issues for smart homes.	Independence Sample T-Test

2 LITERATURE REVIEW

2.1 Internet of Things (IoT)

The IoT deployment process involve technologies such as wireless sensor networks (WSNs), RFID, Bluetooth, wireless fidelity (Wi-Fi), sensors, near field communication (NFC), internet protocol (IP), electronic product code (EPC), and actuators (Bako Ali, 2018).

2.2 Evolution of Internet of Things

The next step for communication between the things (machine to machine) via internet, one of the most talked about and emerging concept today is Internet of Things (IoT) that came with automated features enabling many sectors in automation and helping to ease in each tasks and activities with minimum human intervention (J. Sathish Kumar, 2014).

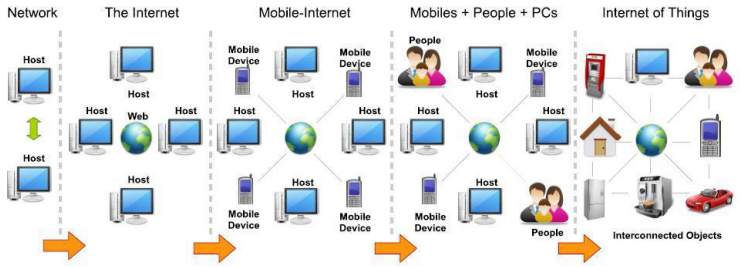


Figure 1: Evolution of IoT (Perera, et al., 2015)

2.3 Internet of Things (IoT) Components

Smart Devices (Things): Smart devices are devices connected with each other in IoT ecosystem. The smart devices are the components of connectivity layer in IoT ecosystem (Rajiv, 2018).

Sensors: The smart sensors collect data in the IoT ecosystem and transfer them to next layer of IoT ecosystem. The various kinds of sensors found in IoT are: temperature sensor, thermostat, humidity sensor, moisture sensor, light intensity detectors, RFID tags, proximity detection, pressure sensor etc (Rajiv, 2018).

Gateway: Gateway ensures the interoperability of connected devices and sensors and manages the data traffic or connectivity between network and protocols. The security administration can be managed in Gateway which acts as a middle layer between cloud and devices (Rajiv, 2018).

Cloud: IoT cloud collects, process, manage the data collected in IoT ecosystem in real time. The IoT cloud integrates the devices, sensors, gateways, protocols, and data storage and can be accessed remotely (Rajiv, 2018).

2.4 IoT in Homes

IoT enabled smart home or smart homes has no any generally accepted definition. A home that equipped with different smart appliances those are capable of exchanging data and information within with the help of internet connection facilitating automation and intelligence to control the various tasks and devices itself is known to be a smart home environment. Smart homes are the demand of this time that studies and surveys has found that IoT devices for smart homes will increase by 53.9% of US households by 2023 (Kozubska, 2019).

2.5 Advantages of Smart Home System

Smart home system has many beneficial advantages having its impacts on our daily life, social causes, organizational development, businesses, health, fitness, scientific research and more. It is no wonder that majority of population today use smart devices and smart home appliances to facilitate them with automations. With the development of the time, today's home is not only the home people live in, but has become the palace of automation with varieties of features. The main advantages the smart home provide are:

- Hands-free convenience
- Automation on home usage such as lights, thermostat, kitchen appliances, outlets, TV, speakers, refrigerators and more
- Energy efficiency
- Enhanced security

- Time savings

2.6 Smart Home Architecture

Generally, smart home architecture comprises service provider, gateway, users and smart devices connected and used in smart home ecosystem. The smart home service can be implemented in various ways. Normally, the smart home service provider hosts the services and users subscribe to use the services. Alternatively, users may purchase each devices, install and use them or can be used in other way by smart hub deployment to control all the devices connected within smart home environment (Geong Sen Poh, 2019).

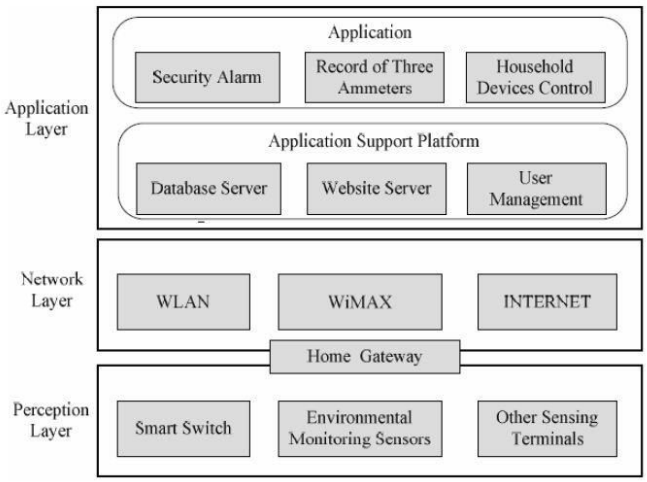


Figure 2: Layer architecture model for IoT based smart home system *(Ali, 2016)*

2.7.3 Security Camera

Security camera is a most important device/smart device in smart home system or used in various security system in industries, offices, and public places. The security camera captures and monitors the activities within its range to maintain security (M. Sathishkumar, 2015). The security cameras that are integrated with the smart home system are prone to various threats and attacks. Although there are different security prevention tools and techniques, the security cameras connected to IoT ecosystem are considered to be less secure than other security cameras.

2.8 Data Privacy Issues in IoT Enabled Smart Home Environment

The IoT devices require user's data and information to function. The protection and awareness of their misuses is the vital factor for every IoT devices users because personal data compromising is of serious concern. The IoT environment has the higher chances of threats and attacks as the environment comprises of personal data and information which are the greater target from insiders as well as outsiders which is one of the key challenges in IoT environment. Even if the personal data and information are encrypted, they are vulnerable to different kinds of threats and attacks and are not safe until they are highly secured. According to FBI report in January 2016, the value of ransom attacks increased to 300% from its previous value which was 42 ransom attacks released in one hour, 1000 in a day, 30000 in a month and 0.36 million in a year on according to report in January, 2015 (Waqar Ali, 2017). CNN has reported that 317 million cyber-attacks occurred on the end of 2016 (Waqar Ali, 2017).

The security concerns that could affect data privacy issues in the IoT ecosystem can be categorized majorly into three different layers. **Front-end sensors and equipment**: unauthorized access to data,

threats to the network, DOS attack; **Network**: unauthorized access to data, network attacks, virus or malware attacks, modification of information, unauthorized access to services; **Back-end of IT system**: safety management of code resources, replacement of operator. The privacy in devices, privacy in communication, privacy in storage, and privacy is processing are the key privacy concern factors of IoT ecosystem (J. Sathish Kumar, 2014). The major threats groups to the IoT enabled smart home environment could be physical attacks, unintentional damage (accidental), disaster and outages, damage/loss (IT assets), failures/malfunctions, eavesdropping/ interception/hijacking, and legal (Dr. Cédric LÉVY-BENCHETON, 2015).

3 RESEARCH METHODOLOGY

3.1 Introduction

Research refers to the re-searching or search for knowledge on specific topic from the previous literature. In other words, searching for knowledge through systematic methods for finding solution to identified problem domain is known as research. The research consists of problem identification, hypothesis formulation, facts and data findings, analyzing, and reaching certain conclusion in the form of solution to problems or gaps identified (Kothari, 2004). Similarly, the methods/techniques used in the research conduction or in research operations by researcher are known as research methods. Likewise, the systematic way of solving the problem through research methods/techniques in research is known as research methodology (Kothari, 2004).

3.2 Research Strategy

Research strategy refers to the plan of action to meet the research goal. In other words, it is referred as the methodological link between philosophy and subsequent way of collecting and analyzing the data by researcher. There are various research strategies such as experiment, survey, archival and documentary, ethnography, action research, grounded theory, narrative inquiry. The survey strategies are generally used for exploratory and descriptive research that allows to collect standardized data from sizable population in highly economical way using questionnaire technique (Mark Saunders, 2016). The strategy helps to collect quantitative data and allows to analyze the data quantitatively using descriptive and inferential statistics. The strategy also allows to deliver the relationship between multiple variables (Mark Saunders, 2016).

Based on the research domain and suitability, the following research has used survey strategy to study the case based on Nepal i.e. the research is primarily based on the primary data sources and partially on secondary data sources. The “case subject” in the case study based of the research topic is “Nepal”. The case study on the case subject refers to in-depth research to generate insight of the subject.

3.3 Research Design

Research design refers to the procedural plan, structure and strategy of investigation focused on the research questions and problem domain identified. It is also known as the plan for data collection and analysis approaches depending upon the purpose of the research. The planning include identification and classification on the sources and approaches of data collection, methods of data collection, selecting respondents for data collection, analysis and evaluation approaches, and justification (Kumar, 2014).

3.5 Data Collection

There are major two data collection approaches for research: primary and secondary. Collecting the data for research need to be adequate and appropriate to the research goals and objectives. Better the

data collection strategy, better will be the final outcome of the research after proper data analysis and evaluation.

Data Sources

Table 17: Data Sources

Primary Data Collection Sources	Secondary Data Collection Sources

• Observation
  ○ Participant observation
  ○ Non-participant observation
• Interview
  ○ Structured Interview
  ○ Unstructured Interview
• Telephone Interview
• Questionnaire
  ○ Open ended
  ○ Close ended
	• Books
	• Journals
	• Reports
	• Newspapers
	• Article
	• Internet
	• Libraries
	• Conference papers

The data collection sources for the following research are primary as well as secondary data sources. The primary data are collected from online survey as well as offline (field) survey using questionnaire methods of data collection while the secondary data sources includes almost every possible sources of data from secondary sources.

3.6 Data Collection Methods

The following research has adopted online and offline (field survey) data collection methods. Questionnaire technique has been used in data collection from online (Google form) and offline (field survey). The online survey was carried out through different methods contacting the respondents through social media platforms such as facebook, instagram, viber, wechat, email etc while offline (field survey) was conducted on general public from different sectors, having students as most of the respondents. Each respondent in the survey was asked to respond on the same set of questions. The questionnaire is developed in listed form in a way that overall questions and their responses cover the research goal, objectives and research questions for the following research. Secondary data are collected from secondary sources such as journals, publications, research papers, books, libraries, and internet source.

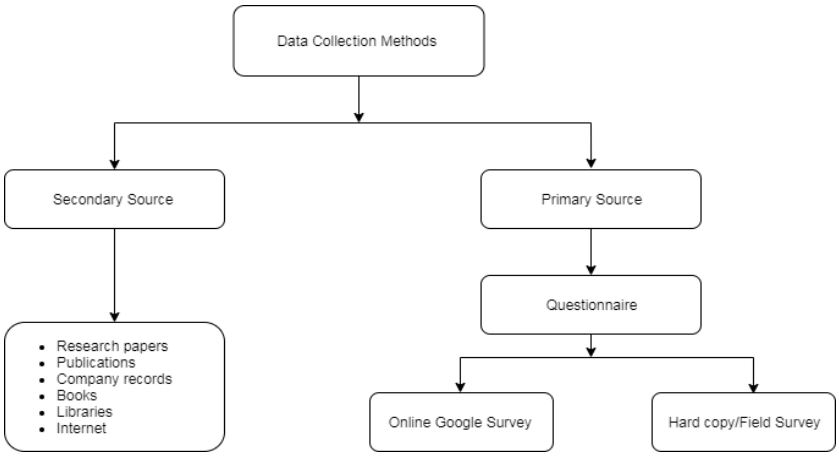


Figure 3: Data Collection Methods

3.8 Sampling Methods

Sample of the research is referred as the group of population or participants selected for the investigation related to the research while sampling is referred as the process of extracting of sample from the population. Generally, there are two sampling method types: Probability sampling methods (random sampling) and Non-probability sampling methods (judgment or non-random sampling) (Alvi, 2016). Sampling method plays a vital role in giving the research output successful and meaningful.

3.9 Sample Size

Table 18: Survey Sample Size

Mode of Distribution of Questionnaire	Distributed	Received
Online	Through Google Online Survey	202
Hardcopy	220	200

3.12 Data Analysis Tool

Data analysis on the collected data from the online as well as offline data collection would be analyzed by IBM SPSS statistics. The data analysis and evaluation on the collected data delivers the analysis among different variables of the research domain. The raw data collected from the survey are organized, coded, categorized, and then presented in tabulation and graphical representation.

3.13 Data Collection Limitations

- The information or response provided by the respondents are based on the respondents' knowledge and experience on the field (IoT and smart homes).
- Every respondent might not be serious on giving genuine response to the questionnaire.
- Some of the questionnaire might not include what the respondents search for to respond.

- Some respondents choose to give different answers to the questionnaire than his/her knowledge and experience.

4 PRESENTATION AND DATA ANALYSIS

4.1 Questionnaire Overview Analysis

The questionnaire prepared for the online and offline survey in the project development are of mixed types. Each question is prepared in a way to cover and have impact on variables of the research. The responses from the questionnaire covers the understanding of technology, usage of technology, comfortability, awareness, importance, knowledge, preparedness relating research domain based on the gender, age and background of the respondents.

4.2 Questionnaire duration

The questionnaire was distributed among online as well as offline (field survey) population which took around a month to complete the survey with 402 respondents in total. The survey could have been possible to collect higher quantity of data but due to the short timeframe of the research, the analysis would be done on the available responses which is fairly a good amount of data for the research.

4.3 Participants

The participants/respondents of the survey are general public having most of them students. The survey was not conducted on the specific group of people because the aim of the research was to get the general public response or general awareness on the technology usage relating research topic to give the best output.

4.4 Methods of Data Analysis

Generally, data analysis and measurement are of three types: nominal, ordinal and scale. Nominal is the most basic level of measurement in data analysis, example – categorical answers such as male/female. Ordinal contains more information than nominal where the answer choices are grouped in ranges such as income bands, age group or rankings. Scale, typically interval scales provide information in depth than nominal and ordinal which is best suited for depth study and data analysis (Statistics Solutions , 2019). Most of the variables in this research are categorical (nominal).

4.4.1 Descriptive Analysis:

Descriptive analysis is used to analyze statistics in summary form to compare and contrast or to find the relationship between variables. The analysis test/techniques the following research uses are given below.

- Frequency distribution in terms of:
  - Smart home understanding
  - Smart home appliances usage
  - Comfortable with smart homes
  - Important to be connected to smart homes
  - Important area like to have control of
  - If smart home usage is safe
- Cross tabulation (Chi-Square Test of Association): The null hypothesis says that there is no significance association between categorical variables. This test (Chi-square test) examines whether the categorical variables has statistical significance association. The result of the test is measured comparing the value (p-value) with 0.05 which states that if the p-value is smaller than 0.05, alternate hypothesis is accepted, means there is a significant association between

variables that are measured. On the other hand, if p-value is greater than 0.05, the alternate hypothesis is rejected (Pandis, 2016).

4.4.1.1 Frequency distribution

The given below statistics and graphical representation shows the frequency on each question from the research questionnaire. The responses and results on the survey are based on the population of Nepal.

How would you describe your understanding of "Internet of Things (IoT)"?

The purpose of this question is to find frequency and percent on what population of the survey participants are familiar with Internet of Things (IoT). It is clear from the results that people somewhat know or finely know about the technology in spite of their usage or comfortability.

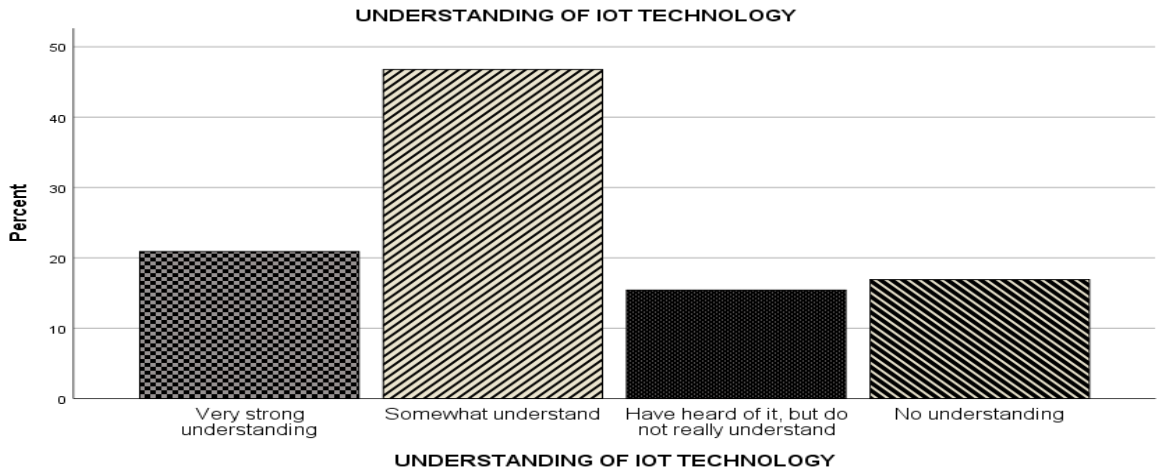
Table 27: Statistics (Understanding of IoT)

Statistics		
UNDERSTANDING OF IOT TECHNOLOGY		
N	Valid	402
	Missing	0
Minimum		1
Maximum		4

Table 28: Understanding of IoT (Frequency/Percent)

UNDERSTANDING OF IOT TECHNOLOGY					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very strong understanding	84	20.9	20.9	20.9
	Somewhat understand	188	46.8	46.8	67.7
	Have heard of it, but do not really understand	62	15.4	15.4	83.1
	No understanding	68	16.9	16.9	100.0
	Total	402	100.0	100.0	

Table 29: Understanding of IoT (Bar Graph)



1. Do you use any smart devices/IoT devices?

The purpose of this question is to find the frequency and percent of respondents those uses smart devices/IoT devices.

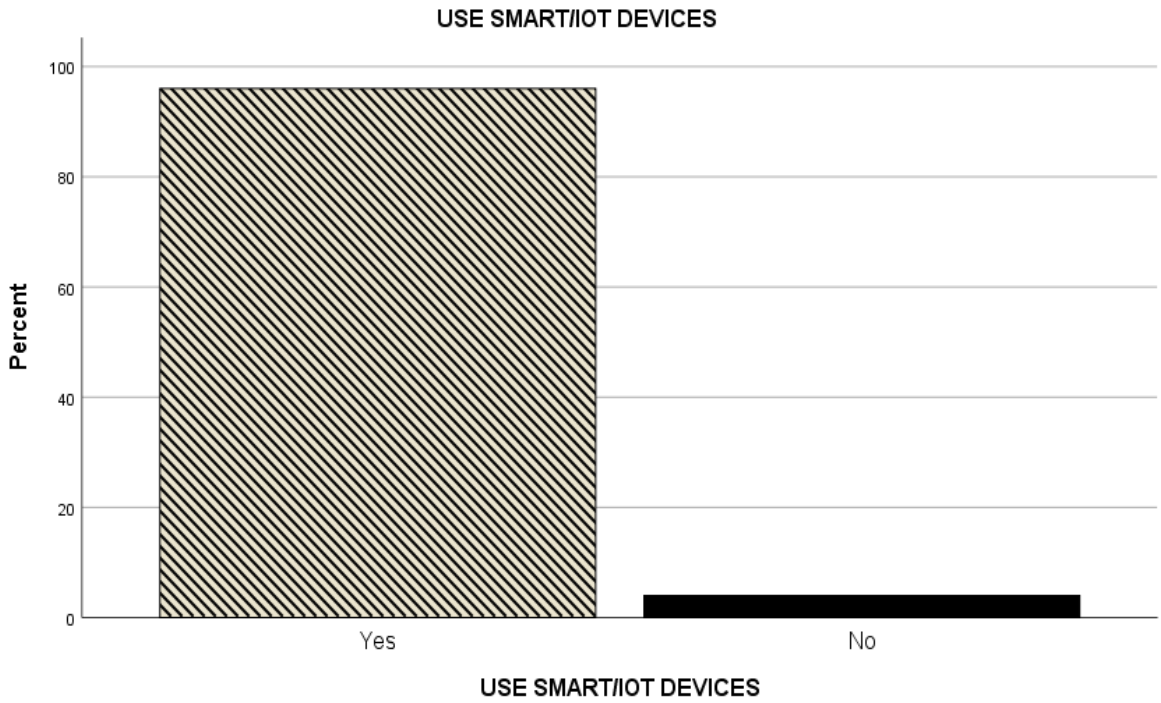
Table 30: Statistics (Use smart/IoT devices)

Statistics		
USE SMART/IOT DEVICES		
N	Valid	402
	Missing	0
Minimum		1
Maximum		2

Table 31: Use smart/IoT devices (Frequency/Percent)

USE SMART/IOT DEVICES					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	386	96.0	96.0	96.0
	No	16	4.0	4.0	100.0
	Total	402	100.0	100.0	

Table 32: Use smart/IoT devices (Bar Graph)



2. How would you describe your understanding of "Smart Homes"?

The question purpose to find the frequency and percent of respondents those who are familiar with smart home systems.

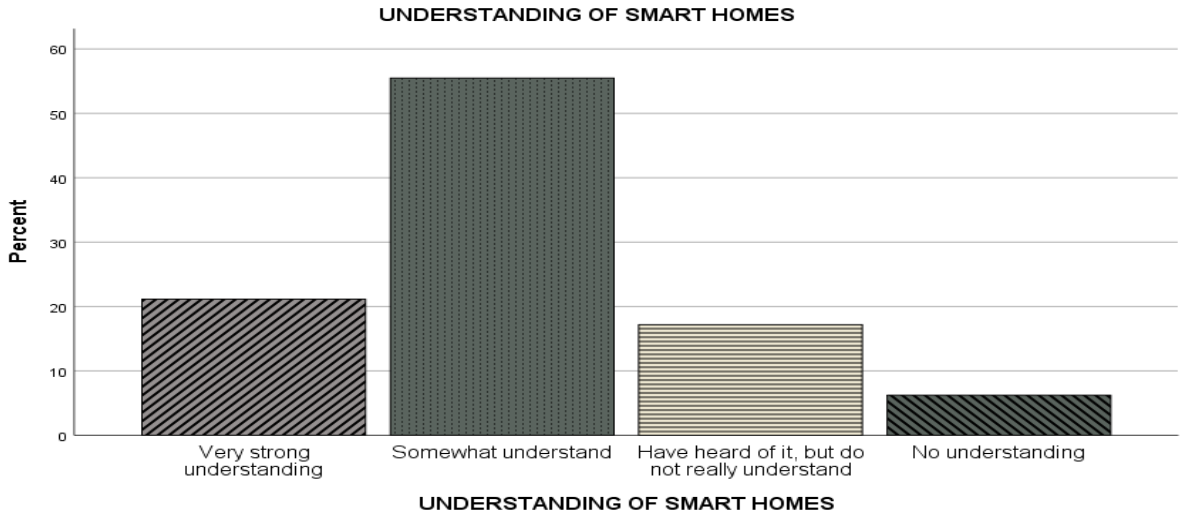
Table 33: Statistics (Understanding of smart homes)

Statistics		
UNDERSTANDING OF SMART HOMES		
N	Valid	402
	Missing	0
Minimum		1
Maximum		4

Table 34: Understanding of smart homes (Frequency/Percent)

UNDERSTANDING OF SMART HOMES					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very strong understanding	85	21.1	21.1	21.1
	Somewhat understand	223	55.5	55.5	76.6
	Have heard of it, but do not really understand	69	17.2	17.2	93.8
	No understanding	25	6.2	6.2	100.0
	Total	402	100.0	100.0	

Table 35: Understanding of smart homes (Bar Graph)



5 SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Discussion and Conclusion

The IoT technology and Smart Homes technology has become so popular topic that they are being the target of intruders and matter of serious concern to stay alert for consumers. The technology has huge coverage and is growing day by day that the researcher has predicted its usage in higher figures than we imagine. At the same time, with the development and its wide coverage, the technology is introducing the more threats and attacks. The smart home usage has added numerous advantages to make the daily doings of human so easier and comfortable. In spite of that, there are also drawbacks of using them due to personal data privacy issues of users which may occur from various threats and security attacks in smart home environment. New security challenges are introducing day by day which has become the

threatening part of smart home environment. Thus, the awareness about its understanding, preparedness, and tackling strategies has become the essential parts for consumers.

5.2 Research Contribution

The research has reflected the current state of Nepal in IoT and smart home understanding along with data privacy awareness on smart home usage. In addition to the secondary data literature study, the research has included data collection from primary sources from the survey conducted on general public in Nepal. The data collected helps to explore the insight knowledge along with the positive as well as challenging factors in smart homes system. Thus, the background understanding and data analysis based on secondary as well as primary data can be utilized for other researches relating this research type. The knowledge on consequences of data privacy issues in smart home ecosystem, their fundamental components to tackle those issues and preparedness can be much beneficial for those who are using, started using, or using in future the smart home systems i.e. the research can be beneficial in social aspects to enhance privacy in smart home ecosystem. In addition, the research can contribute business personnel who are starting or doing business in smart home sectors. Furthermore, as the following research is based on the case study of Nepal, the research can add contribution to the academic researchers who are working on relating topic in Nepal.

5.3 Recommendations

Data privacy is related to data security concerned with proper data handling and keeping data secret from others. Data privacy has become the most important factors in the age of internet to protect us from intruders. There are various places and environments through which the challenges relating data privacy are introduced or happened. Smart home ecosystem has become one of the vulnerable points and target of attacks on data privacy today. Along with facilitated advantages in smart home ecosystem, smart homes have become challenging point for data privacy protection. So, the sufficient security and knowledge on data privacy protection is most essential in smart home environment.

Recommendations for Data Privacy Issues in Smart Homes

Smart home usage can ease the daily doings by its automation feature technology. Many of the organization as well as the home owners has benefited a lot from its facilities. Time save, automation, accuracy, security, remote control are the major benefits the smart technology provides. Despite that, it is also a serious concern to take care of the consequences that may occur by using the technology. So, to enhance the security in IoT ecosystem and smart home environment, following research has summarized the countermeasures and suggestion for smart home users after the careful analysis of smart home environment. The suggestions are quite suitable for the case of Nepal as well as for global perspective.

For Users

Smart homes users themselves are the first party to be aware of smart home usage, its features along with its negative impacts. The fundamental security requirements the customers or users of smart home must follow to avoid different threats and attack in smart home environment are:

1. **Physical security**: The very first thing the smart home users must take care is physical security of smart home appliances to deny the access from outsiders.
2. **Biometric access control**: Access to smart home system and smart home appliances can be protected with biometric access control. By doing so, only the authorized users can access the system.

For Suppliers

The suppliers' duty doesn't limit to providing services or smart home appliances for their customer/consumers. In addition, the suppliers' duty becomes to protect their customers' smart home system from threats and attacks. The research has suggested following points to suppliers so as to maintain the secure smart home systems.

1. **Awareness**: Suppliers must aware their customers about smart home system, usage, and possible threats and attacks in smart home environment.
2. **Default settings**: Suppliers duty include device installation and configurations along with alertness to their customers about default settings in devices. They must suggest their customers to change default settings or change the device settings periodically to prevent vulnerabilities in devices. The rules are implemented in home gateway and internet (Wi-Fi) usage as well which the supplier must aware their customers.

5.4 Limitations

As with all research, the following research also has some limitations. Firstly, during primary data collection, the researcher didn't have access to respondents' devices or smart homes. The research would have been more practical and could have collected real time data if the researcher had got the chance to access and try out their (users) smart home systems. Second, the sample size of the research is small which is not bad but nor good size in the related research domain. If the sample would have been larger, the research could give better output having wide coverage in the research topic. In addition, view from suppliers which is not presented in the research, and also is another limitation of research could have helped the research to be productive from suppliers' perspectives.

5.5 Future Research

The following research helps to enhance the future research to extend the body of knowledge on smart home usage and security countermeasures relating data privacy issues in smart home environment. The research would be much beneficial for academic researchers based on the case study of Nepal as well for the researchers who are working on related research domain. Furthermore, the research findings of the research can be used to propose or develop framework on the data privacy preservation in smart home systems. The following research also would be beneficial for other researchers to explore the dimensions for smart home usage and their data privacy concerns.

5.7 Summary

The main focus of this research was to identify the current state of IoT and smart home understanding and data privacy issues in smart home environment of Nepal. In addition, the research focus to recommend precautions and countermeasure to tackle those data privacy issues in smart home environment. In order to achieve research goals and objective, the secondary data based on the research topic and primary data from survey are collected. After careful analysis on the data collected, the research came up with productive fundamental requirements and knowledge that are required for every smart home user. The research findings and suggestion help smart home users in Nepal to enhance the level of readiness in data privacy issues that may occur in smart home environment. Furthermore, the outcome and recommendations of the research are beneficial for suppliers who are providing smart home services in Nepal.

REFERENCES

Ali, B., 2016. *Internet of Things based Smart Homes: Security Risk Assessment and Recommendations,* Luleå: DiVA portal.

Alvi, M., 2016. *A Manual for Selecting Sampling Techniques in Research,* Munich: Munich Personal RePEc Archive.

Bako Ali, A. I. A., 2018. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *MDPI,* 18(3), p. 17.

Dr. Cédric LÉVY-BENCHETON, M. E. D. M. G. T. D. G. D. D. M. A., 2015. *Security and Resilience of Smart Home Environments ,* s.l.: European Union Agency For Network And Information Security.

Geong Sen Poh, P. G. M. I. ,. J. N., 2019. PrivHome: Privacy-Preserving Authenticated Communication in Smart Home Environment. *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING,* 99(99), p. 13.

J. Sathish Kumar, D. R. P., 2014. A Survey on Internet of Things: Security and Privacy Issues. *International Journal of Computer Applications,* 90(11), p. 7.

Kautish, S., 2008. Online Banking: A Paradigm Shift. E-Business, ICFAI Publication, Hyderabad, 9(10), pp.54-59.

Kautish, S., & Thapliyal, M. P. (2013). Design of new architecture for model management systems using knowledge sharing concept. International Journal of Computer Applications, 62(11), 27–30.

Kautish, S. and Thapliyal, M.P., 2012. Concept of Decision Support Systems in relation with Knowledge Management–Fundamentals, theories, frameworks and practices. International Journal of Application or Innovation in Engineering & Management, 1, pp.1-9.

Kaur, R., & Kautish, S. (2019). Multimodal Sentiment Analysis: A Survey and Comparison. International Journal of Service Science, Management, Engineering, and Technology (IJSSMET), 10(2), 38-58.

Kumar, A., Rajpurohit, V.S. and Kautish, S., 2020. A Study on Technology-LED Solutions for Fruit Grading to Address Post-Harvest Handling Issues of Horticultural Crops. In Modern Techniques for Agricultural Disease Management and Crop Yield Prediction (pp. 203-221). IGI Global.

Kothari, C. R., 2004. *Research Methodology Methods and Techniques.* 2nd ed. New Delhi: New Age International (P) Ltd..

Kozubska, D., 2019. *The Most Promising Areas You Should Focus on as a Home Automation Company,* s.l.: IoT For All .

Kumar, R., 2014. *Research Methodology - a step-by-step guide for beginners.* Fourth ed. London: SAGE Publications Ltd.

LTD, G. B. (., 2018. *Smart House.* [Online]
Available at: https://www.thegabuilders.com/projects/smart-house/
[Accessed 21 August 2019].

M. Bala Krishna, A. V., 2016. *A framework of smart homes connected devices using Internet of Things.* Noida, IEEE.

M. Sathishkumar, S., 2015. Smart Surveillance System Using PIR Sensor Network and GSM. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* 4(1), p. 5.

Mark Saunders, P. L. A. T., 2016. *Research Methods for Business Students.* Seventh ed. England: Pearson Education Limited.

Nepal, H. A., 2019. *Home Automation Nepal.* [Online]
Available at: http://www.homeautomationnepal.com/
[Accessed 21 August 2019].

Pandis, N., 2016. The chi-square test. *American Journal of Orthodontics and Dentofacial Orthopedics ,* 150(5), p. 2.

Rani, S. and Kautish, S., 2018, June. Association Clustering and Time Series Based Data Mining in Continuous Data for Diabetes Prediction. In 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1209-1214). IEEE.
Rajiv, 2018. *What are the major components of Internet of Things,* s.l.: RF Page.

Seaman, J., 2015. Internet of Things: Evolution or Revolution of Technology?. *ISACA Journal ,* Volume 6.

Shafiq Ul Rehman, S. M., 2016. A Study of Smart Home Environment and its Security Threats. *International Journal of Reliability, Quality and Safety Engineering,* 23(3), p. 9.

Statistics Solutions , 2019. *Statistical Analysis: A Manual on Dissertation and Thesis Statistics in SPSS.* [Online]
Available at: https://www.statisticssolutions.com/spss-manual/
[Accessed 03 Nov 2019].

Statistics Solutions, 2019. *Constructing Hypotheses in Quantitative Research.* [Online]
Available at: https://www.statisticssolutions.com/constructing-hypotheses-in-quantitative-research/
[Accessed 4 Oct 2019].

Technology, G. o. N. M. o. C. a. I., 2018. *2018 Digital Nepal Framework - Unlocking Nepal's Growth Potential,* s.l.: Government of Nepal Ministry of Communication and Information Technology.

Waqar Ali, G. D. M. A. M. A. S., 2017. *IoT based smart home: Security challenges, security requirements and solutions.* Huddersfield, UK, IEEE.