

A STUDY ON EMPLOYEE PERCEPTION TOWARDS BYOD AT FABSYS TECHNOLOGIES PRIVATE LIMITED

Submitted in partial fulfillment of the requirements for the award of Degree in

MASTER OF BUSINESS ADMINISTRATION

by

KANIMOZHI.M
Register No.41410158



**DEPARTMENT OF BUSINESS ADMINISTRATION
SCHOOL OF MANAGEMENT STUDIES**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

**Accredited with Grade "A" by NAAC | 12B Status by UGC | Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119**

MAY 2023



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

SCHOOL OF MANAGEMENT STUDIES

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **KANIMOZHI.M 41410158** who carried out the project entitled "**A STUDY ON EMPLOYEE PERCEPTION TOWARDS BYOD AT FABSYS TECHNOLOGIES PRIVATE LIMITED**" under my supervision from January 2023 to March 2023.

DR. PRINCY A S

Internal Guide

External Guide

Dr. BHUVANESWARI .G

Dean – School of Management Studies

SCHOOL OF MANAGEMENT STUDIES
SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(Deemed to be University)
Iyappaar Nagar, Rajiv Gandhi Sala,
Chennai-600 119

Submitted for Viva voce Examination held on 06/05/2023

Internal Examiner

External Examiner

CONSENT & COMPLETION LETTER IN COMPANY LETTER HEAD



Registered Office:

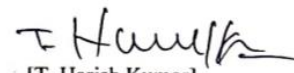
#34/6, Ambal Nagar,
Ekkattuthangal, Chennai,
Tamil Nadu, India. 600032.

30-03-2023

TO WHOM SO EVER IT MAY CONCERN

This is to certify that Ms. KANIMOZHI M, Reg No: 41410158 Final Year student of
MBA (MASTER OF BUSINESS ADMINISTRATION) SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY has Successfully completed her
Project entitled as "A STUDY ON EMPLOYEE PERCEPTION TOWARDS BYOD
AT FABSYS TECHNOLOGIES PRIVATE LIMITED" from January 10th 2023 to
March 30th 2023.

With best regards,


[T. Harish Kumar]
HR-Manager



Web: www.fabsys.in

Ph: 9176471711.

Email: hr@fabsys.in

DECLARATION

I **KANIMOZHI M (41410158)** hereby declare that the Project Report entitled “**A Study on the employee perception towards BYOD at Fabsys Technologies Private Limited**” done by me under the guidance of **DR. PRINCY A S** is submitted in partial fulfillment of the requirements for the award of Master of Business Administration degree.

DATE:05/05/2023

PLACE:Chennai



KANIMOZHI M

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to Board of Management of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my sincere thanks to **Dr. G. Bhuvaneswari, MBA., Ph.D., Dean - School of Management Studies** and **Dr. A. Palani, M.Com., M.Phil., M.B.A., Ph.D., Head - School of Management Studies** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. PRINCY A S** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **School of Management Studies** who were helpful in many ways for the completion of the project.

KANIMOZHI.M

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	(i)
	LIST OF TABLES	(ii)
	LIST OF CHARTS	(iii)
1	INTRODUCTION	
	1.1 .Introduction	1
	1.2 .Industry Profile	3
	1.3 .Company Profile	5
	1.4 .Statement of the problem	9
	1.5 .Objectives of the Study	9
	1.6 .Need for the study	9
	1.7 .Scope & Significance of the study	10
	1.8 Limitations of study	10
2	REVIEW OF LITERATURE	
	2.1 Review of Literature	11
3	RESEARCH METHODOLOGY	
	3.1 Methodology	23
	3.2. Research Design	23
	3.3. Sampling Technique	23
	3.4. Sources of Data	23
	3.5. Structure of Questionnaire	24
	3.6. Sample Size	24
	3.7. Period Of Study	24
	3.8. Location & Targeted people of study	24
	3.9. Hypothesis	24
	3.10. Tools for analysis	25
4	DATA ANALYSIS AND INTERPRETATION	
	4.1 Percentage Analysis	26
	4.2. Anova	50
	4.3. Correlation	51

5	FINDINGS,SUGGESTIONS AND CONCLUSION	
	5.1.Findings of the Study	53
	5.2.Suggestions & Recommendations	54
	5.3. Conclusion	55
	REFERENCES	56
	ANNEXURE I – QUESTIONNAIRE	59
	ANNEXURE II – RESEARCH ARTICLE	64

ABSTRACT

This project titled “A Study on employee perception towards BYOD at Fabsys Technologies Private Limited” aims at understanding the overall effectiveness of using this concept in the corporate world. Bring Your Own Device refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications. This study has a scope to get a better Policy for BYOD implementation in IT Environment. This study enables us to frame an action plan to overcome the security issues and also to show improvement in IT Business Cycle. Multiple choice questions have been chosen to collect the responses from 200 companies. Numerous new findings have been derived from this research has helped to provide few suggestions to the company to improve the employee perception towards BYOD. Bring Your Own Device (BYOD) policy, which allows employees to use their own mobile devices for work and connection to their corporate network, is getting popular in enterprises. While companies want to improve the efficiency and productivity of employees, employees prefer to use their own devices at work, which make them feel more comfortable and free. Although BYOD seems attractive, companies and employees have some security concerns in different and various ways. The aim of this study is to explore employee and organization perspectives about BYOD. It has been found that while organizations and employees’ percept BYOD as having benefits in many ways, their security and privacy concern is a strong barrier on the implementation of BYOD policy. It has been found that while organizations and employees’ percept BYOD as having benefits in many ways, their security and privacy concern is a strong barrier on the implementation of BYOD policy

LIST OF TABLES

TABLE NO	PARTICULARS	PAGE NO
4.1.1	Gender of the respondents	26
4.1.2	Age of the respondents	27
4.1.3	Marital status of the respondents	28
4.1.4	Educational Qualification of the respondents	29
4.1.5	Department of the respondents	30
4.1.6	Experience of the respondents	31
4.1.7	BYOD Implementation in the Organization	32
4.1.8	Type of security risks employees face in BYOD	33
4.1.9	BYOD provides significant move towards safeguarding confidential information	34
4.1.10	Employees comfortability with BYOD in the organization	35
4.1.11	Possible control measures considered for confronting BYOD policies	36
4.1.12	Ineffective management issues resulting in major cause of BYOD security	37
4.1.13	Best mode of approaches in BYOD	38
4.1.14	Characteristics of security models employees use for managing BYOD	39
4.1.15	Satisfaction level of BYOD program in the organization	40
4.1.16	Type of hardware devices employees use under BYOD	41
4.1.17	Organization have proper infrastructure in place to support BYOD	42
4.1.18	Basic control methods employees using for BYOD environment	43

4.1.19	BYOD policy that the Organization follows	44
4.1.20	BYOD management & stipends cost more than company devices	45
4.1.21	BYOD provides right balance between productivity & security	46
4.1.22	Established security procedures to handle BYOD in the organization	47
4.1.23	BYOD program is right fit for the working organization	48
4.1.24	Work tasks employees find useful to do on their own device in BYOD	49
4.2.1	Anova analysis	50
4.2.2	Anova analysis	50
4.3.1	Correlation analysis	51
4.3.2	Correlation analysis	52

LIST OF CHARTS

TABLE NO	PARTICULARS	PAGE NO
4.1.1	Gender of the respondents	26
4.1.2	Age of the respondents	27
4.1.3	Marital status of the respondents	28
4.1.4	Educational Qualification of the respondents	29
4.1.5	Department of the respondents	30
4.1.6	Experience of the respondents	31
4.1.7	BYOD Implementation in the Organization	32
4.1.8	Type of security risks employees face in BYOD	33
4.1.9	BYOD provides significant move towards safeguarding confidential information	34
4.1.10	Employees comfortability with BYOD in the organization	35
4.1.11	Possible control measures considered for confronting BYOD policies	36
4.1.12	Ineffective management issues resulting in major cause of BYOD security	37
4.1.13	Best mode of approaches in BYOD	38
4.1.14	Characteristics of security models employees use for managing BYOD	39
4.1.15	Satisfaction level of BYOD program in the organization	40
4.1.16	Type of hardware devices employees use under BYOD	41
4.1.17	Organization have proper infrastructure in place to support BYOD	42
4.1.18	Basic control methods employees using for BYOD environment	43
4.1.19	BYOD policy that the Organization follows	44

4.1.20	BYOD management & stipends cost more than company devices	45
4.1.21	BYOD provides right balance between productivity & security	46
4.1.22	Established security procedures to handle BYOD in the organization	47
4.1.23	BYOD program is right fit for the working organization	48
4.1.24	Work tasks employees find useful to do on their own device in BYOD	49

CHAPTER 1

INTRODUCTION

1.1. INTRODUCTION

Bring Your Own Device refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications. The term is also used to describe the same practice applied to students using personally owned devices in education settings.

BYOD is making significant inroads in the business world, with about 75% of employees in high growth markets such as Brazil and Russia and 44% in developed markets already using their own technology at work. In most cases, business simply can't block the trend. Some believe that BYOD may help employees be more productive. Others say it increases employee morale and convenience by using their own devices and makes the company look like a flexible and attractive employer. Many feel that BYOD can even be a means to attract new hires, pointing to a survey that indicates 44% of job seekers view an organization more positively if it supports their device.

HISTORY

The term BYOD was mentioned in a paper by Ballagas et al., at UBICOMP 2005. BYOD first entered in 2009, courtesy of Intel when it recognized an increasing tendency among its employees to bring their own devices to work and connect them to the corporate network. However, it took until early 2011 before the term achieved any real prominence when IT services provider Unisys and software vendors VMware and Citrix Systems started to share their perceptions of this emergent trend. BYOD has been characterized as a feature of the "consumer enterprise" in which enterprises blend with consumers. In 2012, the U.S.A Equal Employment Opportunity Commission adopted a BYOD policy, but many employees continued to use their government-issued BlackBerrys because of concerns about billing, and the lack of alternative devices.

NEW TRENDS

The proliferation of devices such as tablets & smartphones, which are now used by many people in their daily lives, has led to a number of companies allowing employees to bring their own devices to work, due to perceived productivity gains and cost savings. The idea was initially rejected due to security concerns but more and more companies are now looking to incorporate BYOD policies, with 95% of respondents to a BYOD survey saying they either already supported BYOD or were at least considering supporting it.

ISSUES

BYOD security relates strongly to the end node problem, wherein a device is used to access both sensitive and risky networks/services. Because of Internet-based risks, some very risk-averse organizations issue devices specifically for Internet use (this is termed Inverse-BYOD). BYOD has resulted in data breaches. For example, if an employee uses a smartphone to access the company network and then loses that phone, untrusted parties could retrieve any unsecured data on the phone. Another type of security breach occurs when an employee leaves the company, they do not have to give back the device, so company applications and other data may still be present on their device.

A key issue of BYOD which is often overlooked is BYOD's phone number problem, which raises the question of the ownership of the phone number. The issue becomes apparent when employees in sales or other customer-facing roles leave the company and take their phone number with them. Customers calling the number will then potentially be calling competitors which can lead to loss of business for BYOD enterprises. International research reveals that only 20% of employees have signed a BYOD policy. If sensitive, classified, or criminal data lands on a U.S. government employee's device, the device is subject to confiscation. A challenging but important task for companies who utilize BYOD is to develop a policy that defines exactly what sensitive company information needs to be protected and which employees should have access to this information, and then to educate all employees on this policy. The USMC is seeking to outsource the security requirements of their BYOD policy to commercial carriers such as Sprint, Verizon,

and AT&T. Another important issue with BYOD is of scalability and capability. Many organizations today lack proper network infrastructure to handle the large traffic which will be generated when employees will start using different devices at the same time. Nowadays, employees use mobile devices as their primary devices and they demand performance which they are accustomed to. Earlier smartphones did not use a lot of data and it was easy for Wireless LAN to handle that amount of data, but today smartphones can access webpages as quickly as most PCs do and have applications that use radio and voice at high bandwidths, hence increasing demand from WLAN infrastructure.

1.2. INDUSTRY PROFILE

Introduction

India is the world's largest sourcing destination for the information technology (IT) industry, accounting for approximately 67 per cent of the US\$ 124-130 billion market. The industry employs about 10 million workforces. More importantly, the industry has led the economic transformation of the country and altered the perception of India in the global economy. India's cost competitiveness in providing IT services, which is approximately 3-4 times cheaper than the US, continues to be the mainstay of its Unique Selling Proposition (USP) in the global sourcing market.

Market Size

The Indian IT sector is expected to grow at a rate of 12-14 per cent for FY2016-17 in constant currency terms. The sector is also expected triple its current annual revenue to reach US\$ 350 billion by FY 2025. India ranks third among global start-up ecosystems with more than 4,200 start-ups. India's internet economy is expected to touch Rs 10 trillion (US\$ 146.72 billion) by 2018, accounting for 5 per cent of the country's GDP. India's internet user base reached over 400 million by May 2016, the third largest in the world, while the number of social media users grew to 143 million by April 2015 and smartphones grew to 160 million. Public cloud services revenue in India is expected to reach US\$ 1.26 billion in 2016, growing by 30.4 per cent year-on-year (y-o-y)[^]. The public cloud market alone in the country was estimated to treble to US\$ 1.9 billion by 2018 from US\$ 638 million in 2014. Increased penetration of internet (including in rural areas) and rapid emergence of e-commerce are the main drivers for continued growth of data center co-location and hosting market in India.

Investments

Indian IT's core competencies and strengths have attracted significant investments from major countries. The computer software and hardware sector in India attracted cumulative Foreign Direct Investment (FDI) inflows worth US\$ 21.02 billion between April 2000 and March 2016, according to data released by the Department of Industrial Policy and Promotion (DIPP).

Some of the major developments in the Indian IT and ITeS sector are as follows:

- Google, the American technology giant, has launched a new Wi-Fi platform called Google station, under which the company will install Wi-Fi hot spots in places frequented by a large number of people like malls, cafes, universities.
- Reliance Industries Ltd (RIL) plans to set up entrepreneurship hubs in key cities and towns, and a Rs 5,000 crore (US\$ 748 million) fund, under the name of Jio Digital India Startup Fund, to invest in technology based startups.
- Apple Inc. plans to set up its first technology development center outside the US in Hyderabad with an investment of US\$ 25 million, which is expected to create 4,500 jobs, as per Mr. Jayesh Ranjan, Secretary, IT for the state of Telangana.
- Wipro Ventures, Wipro's US\$ 100 million corporate venture arm, plans to invest in early-stage Venture Capital (VC) funds based in the US to pursue a strategy of investing/partnering country-focused VCs.

Government Initiatives

Some of the major initiatives taken by the government to promote IT and ITeS sector in India are as follows:

- Mr. Ravi Shakar Prasad, Minister of Communication and Information Technology, announced plan to increase the number of common service centers or e-Seva centers to 250,000 from 150,000 currently to enable village level entrepreneurs to interact with national experts for guidance, besides serving as a e-services distribution point.
- The Government of Telangana has signed an agreement with network solutions giant Cisco Systems Incorporation, to cooperate on a host of technology initiatives, including Smart Cities, Internet of Things, cybersecurity, education digitization of monuments.

- The Pune Smart City Development Corporation (PSCDCL) has signed a memorandum of understanding (MOU) with the European Business and Technology Centre (EBTC), which will allow it to gain access to real-time knowledge of technologies, solutions and best practices from Europe.
- The Human Resource Development (HRD) Ministry has entered into a partnership with private companies, including Tata Motors Ltd, Tata Consultancy Services Ltd and real-estate firm Hubtown Ltd, to open three Indian Institutes of Information Technology (IIITs), through public-private partnership (PPP), at Nagpur, Ranchi and Pune.
- Government of India is planning to develop five incubation centers for 'Internet of Things' (IoT) start-ups, as a part of Prime Minister Mr. Narendra Modi's Digital India and Startup India campaign, with at least two centers to be set up in rural areas to develop solutions for smart agriculture.

1.3. COMPANY PROFILE

Fabsys Technologies private Limited is on the basis of organizing and strengthening the ingredients of an establishment, the crucial factors responsible for objectives. It is formed with a devoted and composite team of professionally qualified, technically proficient, highly experienced members. Combining diverse expertise in business strategy, technology, usability and design, we produce highly scalable business solutions and online positive user experiences. It emphasizes a personal and professional relationship with our clients starting with the initial understanding of client business and requirement. It provides offline and online Data processing and back office support, to create & implement complete IT Enabled Services. It provides the total solutions by bringing together the team with a unified and cohesive approach.

About Technology

Application & Web Servers:

Apache Tomcat, BEA Web Logic Platform.

Relational Database Management Systems (RDBMS):

MySQL, Oracle.

Programming Languages:

Java, C/C++ (including ANSI C, Managed C++, C++/CLI), Scripting Languages (JavaScript, VBScript, Perl, ASP, PHP, JSP, etc.)

Java Technologies: J2EE (EJB, JSP, JDBC, J2ME).

WEB Technologies:

HTTP/HTTPS, HTML/DHTML, XML, XSLT, CSS.

Interactive Design Tools:

Adobe Photoshop, CorelDraw (including Graphic Tools), Corel Photo Paint, Macromedia Flash 8.0.

Services

- Custom Software Development
- Application Development
- Web Application Development
- Enterprise Application Development
- Content Management System
- Ecommerce Solution
- Web Development
- Flash Development
- Web Marketing / SEO
- Software Maintenance
- Content Development Services

Content Writing

Words can create, words can destroy, words can bear revolution. Words express thoughts and emotions. If the right words are not used properly, it can lead to miscommunication. A content-rich website can create a noticeable difference in its ability to bring in traffic. Keyword rich, Innovative design, and understandable content contributes in making a website attractive. An interactive and well written website succeeds in inviting and retaining more traffic. Fabsys is well aware of the importance of content writing and therefore we are trying to offer best quality content writing services at a competitive price.

Project Conceptualization

Drive innovation, validate new product ideas, verify and prototype their potential for customers and investors.

Product Realization:

By combining your products ideas with our delivery capabilities, you can quickly reap time-to-value, offer a more complete product mix and thereby increase your market share and revenue.

- **Independent Quality Assurance & Testing:**

Our Independent Test & Verification service improves quality and reliability of our client's products leading to higher client satisfaction and reduced support costs.

- **Product Maintenance & Customer Support:**

Continuing support and maintenance for new, expanding, and retiring product lines help our clients to retain their customers

- **Product Migration & Software Porting:**

Transition client's products between various platforms and designs helping them enhance their market reach and customer base

- **Professional Services:**

Enhancing our clients service offering through a range of product implementation and support services including Installation, Customization, Integration .

Products

- CRM
- ERP
- SMS Package
- Static Website Development
- Dynamic Website Development
- Flash Website Development
- Online Web Applications
- Academic Projects

Software Development

Fabsys is the fastest growing software development company in India, which offers a wide spectrum of software development services with high level of specialization and deliverable quality to its clients in India. We try hard to deliver superior quality

and cost effective software development solutions to our clients on-time and giving quality outputs to complete customer expectations. Our mission is to enhance the customer satisfaction through providing quality software development services with a team of experienced software developers, who have won the trustworthiness from our clients. We provide software development services through a unique combination of expertise, experience, teamwork and strategic planning.

Website Development

Fabsys is one of the leading and rapidly growing website designing company offering the best and most affordable services like e-commerce web solution, flash web design, custom web design and graphics design for global customers. We deliver high quality web designing services through our motivated and qualified specialist teams which is focused on exceeding clients' expectations every time. We have a team of expert web designer, who have excellent web designing skills to create unique and attractive websites.

- **Discovery** - Understanding your web site goals and audience.
- **Planning** - Establishing timelines, deliverables, and development solutions.
- **Content Architecture** - Planning your website content and structure.
- **Design** - Creating and refining interface and graphic design elements.
- **XHTML Conversion** - After design approved from client side start Coding.
- **Testing** - Testing your web site in multiple browser environments.

Software Development Process:

The first step in software development is analysis. Our Team will make research on the kind of business including the specific needs to achieve your goals. This way, we will be able to establish the perfect software model to be used, that has a tried-and-tested efficiency. After the analysis, the crucial phase comes, when software is designed. In this Phase, the software is put together according to your requirements. It is a very Important step as it is the heart and soul of the whole software development Process. After designing, coding is the next step. In this step, Internet programming languages are put in the equation. It is a highly technical phase but is quite simple with professionals like us. This is main step where Java codes and PHP created. Trial period is the fourth step in software development. In this step, Software engineer as well as the client come together to see if the goals were met.

The software developer will test the codes and the design if they are working and if They really suit the requirements of the possible end-users providing great satisfaction. After testing, the software is set to run. The work will be continuing until software is done. We are willing to provide effective solutions to keep you using the software effectively.

1.4. STATEMENT OF THE PROBLEM

This study is taken how the future of BYOD includes building out policies using Mobile Device Management (MDM) and how it overcomes the challenges in the nature of implementing BYOD in the Organization.

1.5. OBJECTIVES

1.5.1. PRIMARY OBJECTIVES

To study the employee perception towards BYOD (Bring Your Own Device) at Fabsys Technologies Private Limited

1.5.2. SECONDARY OBJECTIVES:

- To study the need for implementing BYOD at Fabsys Technologies Pvt Ltd.
- To study the factors considered for BYOD policy implementation.
- To assess the various security relates issues associated with BYOD.
- To know the efficiency of the BYOD.
- To identify the critical success factors for BYOD implementation.

1.6. NEED FOR THE STUDY:

Mobility is one of the hottest trends in technology, with cell phones, tablets, and other mobile devices being brought to the workplace in ever-increasing numbers. Known as "bring your own device" (BYOD), this change is clearly here to stay. As more employees bring their own mobile devices to work, companies must assess the security risks and costs. By doing nothing, company security is at risk as employee's access email and other potentially proprietary data on their mobile devices. With a policy in place, access to data is controlled, and productivity can be extended to these devices. Through this research, a thorough analysis of the BYOD implementation has to be made to promote the benefits of BYOD to Fabsys. This study will enlighten the readers about the various advantages and the measures to be taken for successful implementation of BYOD at Fabsys.

1.7. SCOPE OF THE STUDY:

- Increase in Productivity and thereby firms profit
- Research enables the company to evaluate the operating efficiency of the BYOD
- New Policy (BYOD) Implementation in IT Environment.
- Strategy for implementation of BYOD by Fabsys Technologies Pvt Ltd in the future
- Action plan to overcome the security issues.
- Improvement in IT Business Cycle.

1.8. LIMITATIONS:

- The study is restricted to only 200 employees of Fabsys Technologies Private Limited.
- The information provided by the respondents could also be biased or inaccurate. No independent verification of the data was possible.
- Time is a major constraint.
- The respondents chosen were busy and have less time to answer the questionnaires.

CHAPTER 2

REVIEW OF LITERATURE

K. G. Gokce & O. Dogerlioglu (2023) This study reviews advantages and disadvantages of using “personally owned device” in the workplace. The research looks at the field from two different perspectives: Employees and managers. Manager perspective is enlightened with the help of interviews. Interview data and literature review provided the basis for the survey instrument which served to learn employee perspective.

Ackerman (2022) Employees and employers have fundamental disagreements on the restrictions that should be placed on personal devices used for work purposes. Employers want to control the devices that connect to their networks, while many employees refuse to allow others privileged access to their personal devices such as admin, root, remote-wipe, or find my iPhone.

Melva Ratchford (2021) conducted a survey on BYOD security issues. Organizations are exposed to new security risks when they allow employees’ personal mobile devices to access the network and the corporate data (a phenomenon called ‘Bring Your Own Device’ or BYOD). They are confronted with inherent security issues that need to be addressed in order to protect the organization and its information. What are the security issues and considerations associated with BYOD environments? With this in mind, the objective of this paper is to present a systematic literature review of scholarly literature (2010–2019) with respect to BYOD security, and to suggest a classification scheme that depicts a holistic approach to securing BYOD environments. The results of this review include the analysis of 38 scholarly articles, where 22 security issues were identified. Based on the proposed classification scheme, the analysis of the findings shows that 86% of the articles identified security issues and considerations associated with the IT domain, 51% identified security issues related to the Management domain, 45% related to the Users domain, and 19% related to the Mobile Device domain. The results also show that BYOD security issues corresponding to policies are among the most frequently addressed concerns, followed by network security, data protection, user’s attitude/behavior and governance.

U. Vignesh, S. Asha (2021) conducted a survey about Modifying Security Policies Towards BYOD in the IT Consumerization phase, the organizations permit their

employees to bring their personally owned device to workplace. This is achieved through enforcing policy or agreement - Bring Your Own Device. The BYOD policies adopted in numerous organizations are vague and generally immature. The prevailing security policies in BYOD are no more supportive for mobile devices like smartphones, tablets and laptops. The security policies must be modified to suit these devices. To mitigate this downside, 3-tier enhanced policy architecture is proposed which specifies the policies to be followed by the device, applications and organizations.

Bashayer Alotaibi, Haya Almagwashi (2018) tells about the survey regarding A Review of BYOD Security Challenges, Solutions and Policy Best Practices 2018. Recently, many employees' own smartphones and tablets; where they use these devices in the workplace either for personal use or to perform functional tasks. Perhaps this considered as the main motivation for numerous organization to pay attention to 'bring your own device' business trend; which is related to the use of personal devices for business purposes. For an organization, this brings some opportunities and security risks. The establish of BYOD policies always be a tough task, as an organization needs to avoid security risks and increase employee productivity. However, the associated security risks with BYOD policy can be managed by developing an effective security policy and adopt some technical security control and procedures. This research paper covers the review of current BYOD security challenges and issues, security solutions and policy best practices in organizational perspective. Moreover, a comprehensive security policy model presented and discussed.

Sara Ali, Muhammad Nauman Qureshi & Abdul Ghafoor Abbasi (2015). This study tells about The trend of adapting BYOD or "Bring Your Own Device" concept in enterprise environment is increasing due to mutual benefits that the company and employees get. Organizations get benefit of increased productivity and reduced IT expenditure whereas the employees are able to use the mobile device which is comfortable and convenient for them. However, BYOD deployment brings serious security and privacy concerns. Critical information of organizations can be leaked if proper measures are not taken to secure BYOD devices. Moreover, if due to BYOD model, customer's data gets lost or compromised then the company's reputation and trust relationship might get damaged. This paper analyzes threats associated with BYOD, presents security requirements and provides classification of BYOD

security models as discussed in literature till date. Based on the identified gaps, it further provides a comprehensive design which meets the basic security requirements for BYOD paradigm. The proposed framework does not require modification to the underlying kernel and allows the IT administrator to remotely manage and control BYOD devices.

Vignesh, U., & Asha, S. (2015) Modifying security policies towards BYOD. In the IT Consumerization phase, the organizations permit their employees to bring their personally owned device to workplace. This is achieved through enforcing policy or agreement - Bring Your Own Device. The BYOD policies adopted in numerous organizations are vague and generally immature. The prevailing security policies in BYOD are no more supportive for mobile devices like smartphones, tablets and laptops. The security policies must be modified to suit these devices. To mitigate this downside, 3-tier enhanced policy architecture is proposed which specifies the policies to be followed by the device, applications and organizations.

Meisam Eslahi; Maryam Var Naseri; H. Hashim; N.M. Tahir; Ezril Hisham Mat Saad (2014) conducted a survey on BYOD Current state and security challenges 2014 Recently, BYOD or Bring Your own Device has become one of the most popular models for enterprises to provide mobility and flexibility in workplaces. The emergence of new technologies and features of mobile devices makes them integral parts of every aspect of daily business activities. Also, mobile networks are now well integrated with the Internet (e.g. 3G, 4G and LTE technologies), therefore, in BYOD, the personal devices (i.e. mobile devices) can be used to increase employees' satisfaction and reduce an organization's device costs. Mobile devices are not well protected compared to computer and computer networks and users pay less attention to security updates and solutions. As a result, mobile security has become a crucial issue in BYOD as employees use their own mobile devices to access an organization's data and systems. Therefore, in this paper we present an overview of the current state of BYOD security and we discuss some future challenges in this area.

Hormazd Romer (2014) Best practices for BYOD security IT revolutions tend to be double-edged swords. There are always benefits – increased computing power or mobility or ease-of-use or some exciting combination of features that might have seemed unimaginable just a few years earlier. Inevitably however, these new features and benefits also bring new difficulties and risks. To assess the risks of

BYOD computing, we need to consider everything from data contamination to user habits to the activities of criminal syndicates.

Mitrovic, Z., Veljkovic, I., Whyte, G., & Thompson, K. (2014) Introducing BYOD in an organization with the recent technology advances and the rapid adoption of tablet computers and smartphones, it has become increasingly common for employees to use their own personal devices to perform various tasks in their work-place. This phenomenon is better known as Bring Your Own Device (BYOD). This new concept is seen as twofold: as not that simple to handle and, at the same time, many organizations are quickly adopting BYOD as it has been shown that it offers many positive effects such as increased job satisfaction, employee morale, better productivity and consumer services. However, permitting employees to utilize their own device of preference in the work-place also brings some risks often associated with the loss of control over organizational data. Hence, this study set to determine and assess the risk of introducing BYOD in an ICT organization. The Case Study approach elicited that the secure use of the BYOD requires the introduction of mixed measures: technical (e.g. Mobile Device Management - MDM) and non-technical (e.g. ICT or BYOD security policies). This study also explored the customer services view related to the BYOD initiative and suggests that use of this initiative can leverage services. The contribution of this study, aimed at practitioners and academics, is seen as threefold as it can help organizations to successfully manage the introduction of BYOD for employees and customer's satisfaction, create and implement appropriate policies and also assist the individuals to learn about the risks related to the use of BYOD in an organization.

Armando, A., Costa, G., Verderame, L., & Merlo, A. (2014) Securing the "bring your own device" paradigm The current mobile application distribution model cannot cope with the complex security requirements of the emerging "bring your own device" (BYOD) paradigm. A secure metamarket architecture supports the definition and enforcement of BYOD policies and offers a promising prototype implementation tested under realistic conditions. An experimental test using the US government's BYOD security policy was conducted on 860 applications found in the Android store with three main policy rules; (a) applications cannot save files locally to the device, (b) once applications are terminated the temporary data must be deleted, and (c) Bluetooth data transfers are restricted. The results provided evidence that the implementation of a security layer has a minimal impact on the performance of the

device and that the code enforcements to restrict the storage of files locally or transfer of files via Bluetooth were effective. This article is useful for this specific research study because it delivers potential risk mitigation strategies available for implementation into an organization's BYOD policy, along with third party vendors that have created products that may assist in developing IDENTIFYING BEST PRACTICES FOR A BYOD POLICY 28 and executing these strategies. The results of the experimental prototype indicate that a set of security controls installed correctly may mitigate data loss with minimal degradation in performance on the mobile device.

Chang, J. M., Ho, P.-C., & Chang, T.-C. (2014) Securing BYOD. IT Professional Today's IT departments are concerned with the popularity of BYOD, because mixing personal and enterprise data presents security threats to corporate proprietary information. IT departments must develop company security policies that let employees access sensitive resources using personal devices. Summary. The article created by Chang et al. examines the challenges faced within IT departments with respect to BYOD practices and proposed solutions. In the article, security issues, malicious software, and management on the device were declared as a few of the challenges. The authors utilized studies and surveys conducted by organizations such as Intel, IBM, Webroot, Sophos, Ubuntu, and the U.S. White House. The results of each study/survey articulated the desire of employees for BYOD and the challenges facing the IT departments who have to regulate BYOD. Chang et al. covered possible solutions such as mobile device management (MDM), mobile application management (MAM), and mobile content management (MCM) tools. They conclude the article with the assertion that a BYOD policy is required in order to maintain security control over company data and in the long run promote a positive ROI. The technologies used to enforce the policies should be carefully evaluated based on performance, separation of personal and organizational data, usability, and enforceability

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014) Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap The purpose of this study is to examine the factors that determine whether employees follow Bring Your Own Device (BYOD) policies through the lens of the Protection Motivation Theory. BYOD is rapidly becoming the norm rather than the exception. As a result, firms are establishing

BYOD policies to address the risk inherent in allowing individuals to use their own devices to access or store company data. This paper reports the results of a survey of accounting students, non-accounting students, and full-time employees. Results demonstrate that participants' intentions to comply with a BYOD policy were primarily motivated by Self Efficacy and Response Efficacy. Further, Threat Severity was more salient for accountants than non-accountants, perhaps due to their sensitivity to confidential data. Finally, when actual compliance behavior was considered, costs to comply were much more salient to employees and could be strong deterrents to full compliance. These findings have important theoretical and practical implications.

Webroot. (2014) Fixing the disconnect between employer and employee for BYOD (bring your own device). It's no surprise that there are many articles and papers on Bring Your Own Device (BYOD) that will advise employers on how to secure employee devices. Webroot believes there is a large disconnect between how employees are using mobile security and the ways that organizations are implementing BYOD. Before conflicts start to erode the considerable gains BYOD brings to both parties, we are uncovering the realities of this disconnect to better inform employers on how to work with employees using personal or employer issued devices. To explore this disconnect, Webroot commissioned a two-part research survey looking at employee and employer BYOD attitudes and concerns around securing personal mobile devices. There is also evidence that employers often only pay lip service to consulting with employees over BYOD security. This can create problems given the large number of personal devices being used for work purposes. As a result of these research surveys, Webroot has developed an employee BYOD Bill of Rights. This tool serves as a guideline that employers can use to help bridge the security gap between employees' preferences and the security requirements of their organizations.

Crossler et al. (2014) This study employed the protection motivation theory (PMT) to create hypotheses about whether or not the student/employee intended to or would actually comply with the BYOD policy. This article is useful for this specific research study because it assists in identifying the best delivery methodology for end user BYOD processes, procedures, and policies to provide the highest possible positive returns.

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness Smartphone information security awareness describes the knowledge, attitude and behaviour that employees apply to the security of the organisational information that they access, process and store on their smartphone devices. The surge in the number of smartphone devices connecting to organisational systems and used to process organisational data has enabled a new level of operational efficiency. While employees are aware of the benefits they enjoy by bringing their personal devices into the workplace, managers too are aware of the benefits of having a constantly connected workforce.

Disterer et al. (2013) This article demonstrates the explosive growth in the use of mobile devices and highlights the trend of integrating the use of the devices directly into the professional lives of individuals. As the use of mobile devices is ingrained into the daily lives of employees, employees are returning with the plea to work from a single device instead of having one for work and one for personal use. The article articulates the risks associated with BYOD opportunities and the complexity of implementing a BYOD policy. Regardless of the solution, policies for the associated platform and device are required for secure use, such as a policy stating that the device must not be compromised by malware, remote wipe capabilities must be available if data is stored locally.

Khoula AlHarthy, Wael Shawkat (2013) Implement network security control solutions in environment Bring Your Own Device (BYOD) security is the way to protect organization's network against Variety of threats which come through mobile devices and access channels. This research paper explains the implementation of BYOD security solution in higher education institution in Oman. This security solution will help to protect the network data from unauthorized access, as well as, controlling unmanaged devices which are smartphones and mobile devices. This research will follow these steps starting with literature review, data collection, analysis, design the network structure with suggested solution and implementation for BYOD security solutions. As well as, monitoring the network performance with the implanted solutions to keep track if traffic flow with high availability and security. This research paper will help to facilitate the work to the network users through allowing BYOD as well as increase the network availability, ability and security through 802.1x, CA and Radius.

Bill_Morrow (2013) BYOD security challenges: control and protect your most sensitive data Several new trends in information access are impacting organizations' ability to control and secure sensitive corporate data. The increase in web applications, cloud computing and Software as a Service (SaaS) offerings, and the Bring Your Own Device (BYOD) phenomenon, means that employees, business partners and customers are increasingly accessing information using a web browser on a device not owned or managed by the organization. The increase in web applications, cloud computing and Software as a Service (SaaS) offerings, and the Bring Your Own Device (BYOD) phenomenon are driving employees, business partners and customers to increasingly access information on devices are not managed by IT departments. This has resulted in security implications for data leakage, data theft and regulatory compliance. To protect valuable information, organizations must stop making a distinction between devices in the corporate network and devices outside of it, argues Bill Morrow of Quarri Technologies.

Aaron M. French, Chenggi Guo, J P Shim (2013) This paper summarizes the panel discussion that occurred on the 2013 Americas Conference on Information Systems to discuss the current status, issues, and future direction of the use and adoption of bring your own device (BYOD). BYOD is widely used around the world. The invited panelists comprised five faculty members from the United States and Korea specializing in information systems. The covered BYOD topics included current use, real-world cases, adoption, pros and cons, issues (cultural, security, privacy), and future directions. The panel also covered bring your own service (BYOS) and bring your own apps (BYOA).

Georg Disterer 2013 BYOD Bring Your Own Device Using modern devices like smartphones and tablets offers a wide variety of advantages; this has made them very popular as consumer devices in private life. Using them in the workplace is also popular. However, who wants to carry around and handle two devices; one for personal use, and one for work-related tasks? That is why "dual use", using one single device for private and business applications, may represent a proper solution. The result is "Bring Your Own Device," or BYOD, which describes the circumstance in which users make their own personal devices available for company use. For companies, this brings some opportunities and risks. We describe and discuss organizational issues, technical approaches, and solutions.

Ackerman, E. (2013) The bring-your-own-device dilemma The smartphone revolution opened the floodgates to the BYOD (bring your own device) trend among workers. Carrying two devices is cumbersome, and many people simply preferred to use their new devices over corporate- issued phones or laptops. Ackerman's article describes the dilemma that IT departments are facing. The main approach to the information Ackerman The article also highlights an investigation into the BYOD rollout program at Intel, which worked gathered is through empirical analysis of other case studies and surveys towards a compromise with their employees to encourage secure technology habits. This article is useful for this specific research study because it provides a concrete example of the benefits of an organizational BYOD policy in the form of soft ROI benefits created by greater employee efficiency in their daily lives.

Fiorenza, P. (2013) Mobile technology forces study of bring your own device with employee mobility transitioning from an amenity to a necessity in today's workplace, there has never been a higher demand for mobile technology. Due to emerging organizational pressures to implement a mobile strategy, GovLoop recently partnered with Cisco Systems Inc. to explore one of the most pressing and important trends facing government today: how to effectively -- and securely -- implement a bring your-own-device (BYOD) initiative. Their research is presented in a report, Exploring Bring Your Own Device in the Public Sector. The report is an important read for any organization considering implementing a BYOD program at their agency. It is a practical, hands-on guide to help agencies craft a BYOD strategy. The survey -- administered to the GovLoop community -- was designed to understand the common challenges and roadblocks for BYOD adoption in the public sector.

Disterer, G., & Kleiner, C (2013) BYOD Bring your own device. Procedia Technology Using modern devices like smartphones and tablets offers a wide variety of advantages; this has made them very popular as consumer devices in private life. Using them in the workplace is also popular. However, who wants to carry around and handle two devices; one for personal use, and one for work-related tasks? That is why "dual use", using one single device for private and business applications, may represent a proper solution. The result is "Bring Your Own Device," or BYOD, which describes the circumstance in which users make their own personal devices available for company use. For companies, this brings some

opportunities and risks. We describe and discuss organizational issues, technical approaches, and solutions. Summary. This article demonstrates the explosive growth in the use of mobile devices and highlights the trend of integrating the use of the devices directly into the professional lives of individuals. As the use of mobile devices is ingrained into the daily lives of employees, employees are returning with the plea to work from a single device instead of having one for work and one for personal use. The article articulates the risks associated with BYOD opportunities and the complexity of implementing a BYOD policy.

Ghosh, A., Gajar, P. K., & Rai, S. (2013) Bring your own device (BYOD): Security risks and mitigating strategies. The growth of mobile technology, with regard to availability of 3G/4G services and devices like Smartphone's has created new phenomenon for communication IDENTIFYING BEST PRACTICES FOR A BYOD POLICY 33 and data processing ability to do business. One such phenomenon that has emerged in the business environment is BYOD (Bring Your Own Device), which means that employees use their personal device to access company resources for work, inside or outside organizational environment. This new phenomenon brings with itself new opportunities but has many risks associated with it. Using mobile devices for personal as well as professional work brings with itself risks that need to be mitigated. The aim of this work is to provide various mobility strategies, defenses and measures, control aspect, management and governance aspect to look forth in implementing a BYOD strategy in an organization. The BYOD concept was not possible until the realization of further advancements in mobile network connectivity, easier accessibility of company applications through the web, and the increased processing power of mobile devices. Benefits of BYOD range from improved employee morale to reduction in user training when implementing a BYOD policy, but BYOD does not come without additional risks and other challenges. The article introduces four security strategies: (a) here is your own device (HYOD), a complete company-provided solution including the device and support; (b) choose your own device (CYOD), a company-provided solution that allows the end user to select the device; (c) bring your own device (BYOD), where employees purchase their own device and employer policies for use must be followed; and (d) on your own device (OYOD), a solution in which employees own their devices but the organization does not provide support or policies for device use.

Ghosh et al (2013) identify the growing push of employees who wish to use their personal devices for work purposes. The BYOD concept was not possible until the realization of further advancements in mobile network connectivity, easier accessibility of company applications through the web, and the increased processing power of mobile devices. Benefits of BYOD range from improved employee morale to reduction in user training when implementing a BYOD policy, but BYOD does not come without additional risks and other challenges.

Johnson, K. & Filkins, B.L. (2012) BYOD security survey Mobile devices are more pervasive in businesses today than in previous generations of computing (desktops and laptops). Mobile apps on these devices are used for both personal and business purposes. According to the International Association for the Wireless Telecommunications Industry (CTIA) report released in the fourth quarter of 2011, there were more mobile devices in the United States than people! These devices and their apps have become foundational tools for today's workforce, and they are more complex in their operating systems, security, use cases and ownership. They are being integrated into the daily business processes and operations of organizations, improving productivity and becoming a critical, yet complex, component of the computing environment. At the same time, mobile devices have become more and more powerful, often exceeding PC performance, app diversity and capabilities found in organizations today. Smart devices have also caught the attention of attackers who are now commonly targeting their rich apps and their access to even more valuable backend data such as bank accounts, corporate (organizational) intellectual property and personal health information.

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. Clearly, there are several important advantages for employees and employers when employees bring their own devices to work. But there are also significant concerns about security privacy. Companies and individuals involved, or thinking about getting involved with BYOD should think carefully about the risks as well as the rewards. The authors predict that the next generations will expect BYOD policies in place to protect their security when using personal devices for professional purposes. This article is useful for this specific research study because it defines the dual nature of the risks associated with BYOD policies: the protection of the organization's data and networks, and the privacy and security of the employee's information on the device. Separation and security of the two sets of

information is a concern that should be considered in a BYOD policy. Miller et al. (2012) remind employers that desire BYOD practices that BYOD security concerns are very similar to the security concerns that were identified when laptops first became popular.

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. Clearly, there are several important advantages for employees and employers when employees bring their own devices to work. But there are also significant concerns about security privacy. Companies and individuals involved, or thinking about getting involved with BYOD should think carefully about the risks as well as the rewards.

Johnson, K. & Filkins, B.L. (2012) Mobile devices are more pervasive in businesses today than in previous generations of computing (desktops and laptops). Mobile apps on these devices are used for both personal and business purposes. According to the International Association for the Wireless Telecommunications Industry (CTIA) report released in the fourth quarter of 2011, there were more mobile devices in the United States than people! These devices and their apps have become foundational tools for today's workforce, and they are more complex in their operating systems, security, use cases and ownership. They are being integrated into the daily business processes and operations of organizations, improving productivity and becoming a critical, yet complex, component of the computing environment.

CHAPTER 3 RESEARCH METHODOLOGY

3.1. METHODOLOGY:

Research methodology is the description, explanation, and justification of various methods of conducting research. Methodology is defined as the study of methods by which we gain knowledge; it deals with the cognitive processes imposed on research by problems arising from the nature of its subject matter. It is the procedure which researcher can go about their work of description, explanation, and predicting phenomena. For the study on employee perception towards BYOD at Fabsys Technologies Private Limited, the following research plan has been formulated and executed.

3.2. RESEARCH DESIGN:

The study is descriptive in nature. This research is basically fact finding with adequate interpretation using simple analysis of data and by developing thinking and elaborating of patterns and obtaining tentative generalizations as hypothesis.

3.3. SAMPLING TECHNIQUE:

Random sampling method

A Random sample is one of the main types of probability sampling methods. A convenience sample is a sampling method that allows for the randomization of sample selection or randomly selects a subset of participants from a population.

3.4. SOURCES OF DATA:

Data collection is the term used to describe a process of preparing and collecting data.

PRIMARY DATA:

In primary data collection, you collect the data yourself using methods such as interviews and questionnaires. The key point here is that the data you collect is unique to you and your research and, until you publish, no one else has access to it.

SECONDARY DATA

Secondary data is data collected by someone other than the user. Common sources of secondary data for social science include censuses, surveys, organizational records and data collected through qualitative methodologies or qualitative research.

3.5. STRUCTURE OF QUESTIONNAIRE:

Questionnaire was divided into two sections. First part was designed to know the general information about Employees and the second part contained the **employees' perceptions towards BYOD at Fabsys Technologies Private Limited.**

3.6. SAMPLE SIZE:

A Sample size of 200 employees in Fabsys Technologies Private Limited are taken to be the Sampling in wide area.

3.7. PERIOD OF STUDY:

The study was conducted for the period of 90 days.

3.8. LOCATION & TARGETED PEOPLE OF STUDY:

This study was carried out in Fabsys Technologies Private Limited located in Chennai and the employees of this company are the target people of this study.

3.9. HYPOTHESIS:

- **HYPOTHESIS -1**

Ho: There is no significant relationship between various department and positive influence of BYOD in the firm.

H1: There is a significant relationship between various department and positive influence of BYOD in the firm.

- **HYPOTHESIS-2**

Ho: There is no significant relationship between experience and work tasks assigned to the employees under BYOD policy.

H1: There is a significant relationship between experience and work tasks assigned to the employees under BYOD policy.

3.10. TOOLS FOR HYPOTHESIS

Simple percentage analysis, Anova and Correlation are used for this study to verify the data.

3.10.1. PERCENTAGE METHOD

In mathematics, a percentage is a number or ratio expressed as a fraction of 100. It is often denoted using the percent sign, "%", or the abbreviation "pct."; sometimes the abbreviation "pc" is used in the case of quantities in economics. A percentage is a dimensionless number (pure number). The percentage is used for making comparison between two or more series of data and to know the accurate percentage of data collected. Here simple percentage method is used. The formula for percentage method is as follows:

Percentage of respondents = (number of respondents ÷ total number of respondents) × 100

3.10.2 ANOVA

Essentially, ANOVA in SPSS is used as the test of means for two or more populations. ANOVA in SPSS must have a dependent variable which should be metric (measured using an interval or ratio scale). ANOVA in SPSS must also have one or more independent variables, which should be categorical in nature.

3.10.3 CORRELATION

Correlation in SPSS is a statistical technique that shows how strongly two variables are related to one another or the degree of association between them. It is a technique that shows how strongly two variables are related to each other or the degree of association between the two variables.

CHAPTER 4

DATA ANALYSIS AND INTERPRETATION

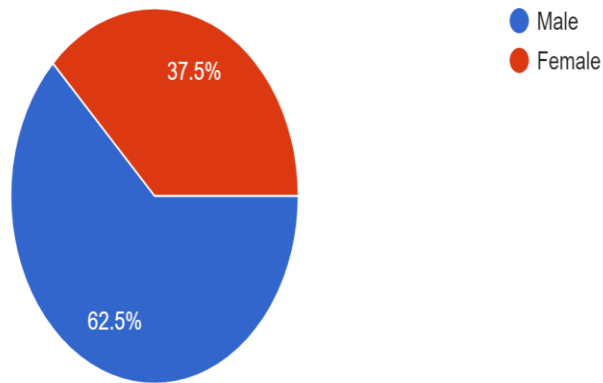
4.1. PERCENTAGE ANALYSIS

TABLE: 4.1.1 Gender of the respondents

GENDER	NO.OF.RESPONDENTS	PERCENTAGE
Male	125	63%
Female	75	37%
TOTAL	200	100

CHART: 4.1.1 Gender of the respondents

Gender
200 responses



INTERPRETATION

From the above table it is interpreted that the number of male respondent is 63% and female respondent is 37%.

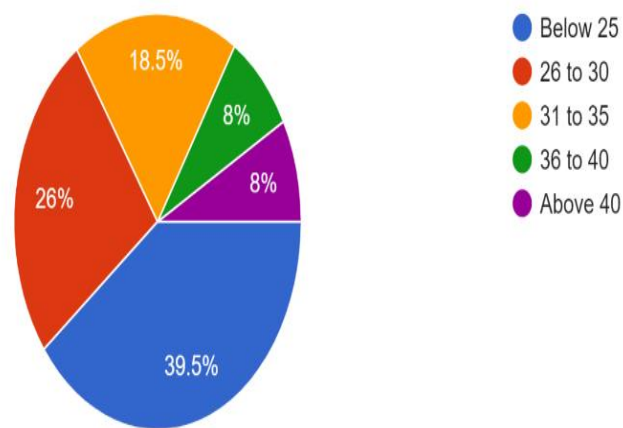
TABLE: 4.1.2 Age of the respondents

AGE	NO.OF.RESPONDENTS	PERCENTAGE
Below 25	79	40%
26 to 30	52	26%
31 to 35	37	18%
36 to 40	16	8%
Above 40	16	8%
TOTAL	200	100

CHART: 4.1.2 Age of the respondents

Age (in Years)

200 responses



INTERPRETATION

From the above table, it is interpreted that the 40% of the respondents are belong to the age group of Below 25 years category, between 26 to 30 age of the respondents are 26%, between 31 to 35 age of respondents are 18%, between 36 to 40 age of the respondents are 8% and above 40 age of the respondents are 8%.

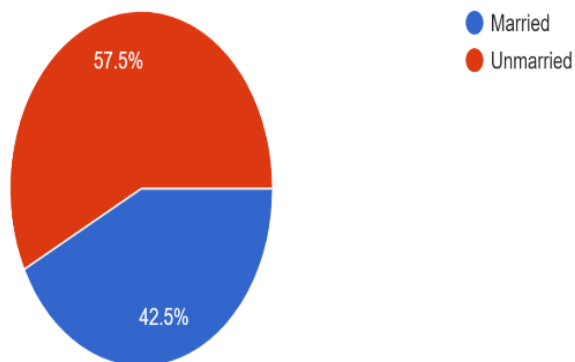
TABLE: 4.1.3 Marital status of the respondents

MARITAL STATUS	NO.OF.RESPONDENTS	PERCENTAGE
Married	85	42%
Unmarried	115	58%
TOTAL	200	100

CHART: 4.1.3 Marital status of the respondents

Marital status

200 responses



INTERPRETATION

From the above table, it is interpreted that the 42% of the respondents are Married and 58% of the respondents are unmarried.

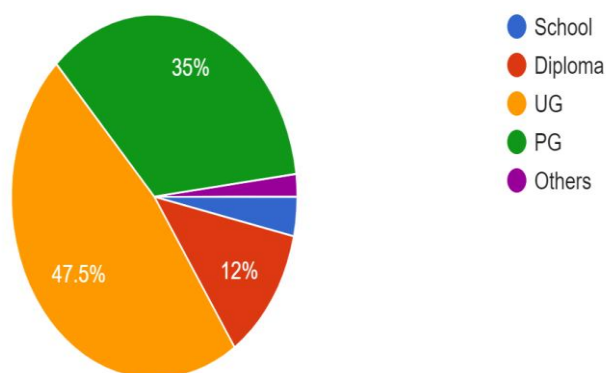
TABLE: 4.1.4 Educational Qualification of the respondents

EDUCATIONAL QUALIFICATION	NO.OF.RESPONDENTS	PERCENTAGE
School	07	3%
Diploma	24	12%
UG	95	48%
PG	70	35%
Others	04	2%
TOTAL	200	100

CHART: 4.1.4 Educational Qualification of the respondents

Educational Qualification

200 responses



INTERPRETATION

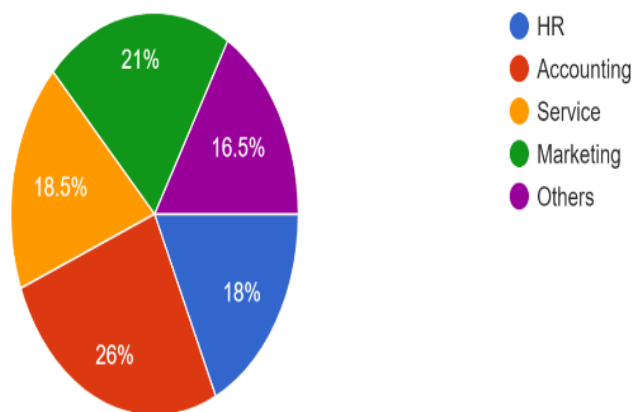
From the above table, it is interpreted that the educational qualification of the respondents 3% of the respondents are belong to School level educational qualification, 12% of the respondents are belong to Diploma educational qualification, 48% of the respondents are belong to UG educational qualification, 35% of the respondents are belong to PG educational qualification and 2% of the respondents are belong to other educational qualification.

TABLE: 4.1.5 Department of the respondents

DEPARTMENT	NO.OF.RESPONDENTS	PERCENTAGE
HR	36	18%
Accounting	52	26%
Service	37	19%
Marketing	42	21%
Others	33	16%
TOTAL	200	100

CHART: 4.1.5 Department of the respondents

Department
200 responses



INTERPRETATION

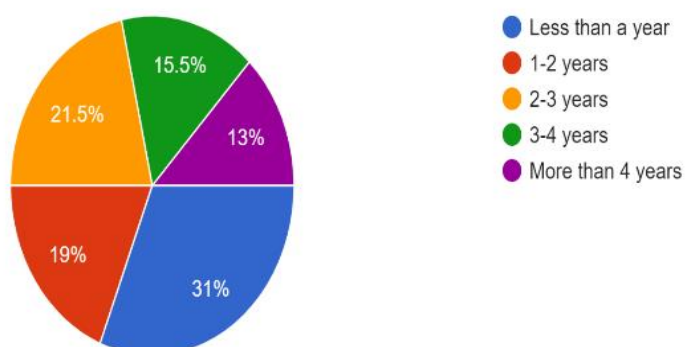
From the above table, it is interpreted that the Department of the employees. 18% of the respondents are belong to the HR Department, 26% of the respondents are belong to Accounting Department, 19% of the respondents are belong to Service Department, 21% of the respondents are belong to Marketing Department and 16% of the respondents are belong to Other Department.

TABLE: 4.1.6 Experience of the respondents

EXPERIENCE	NO.OF.RESPONDENTS	PERCENTAGE
Less than a Year	62	31%
1-2 Years	38	19%
2-3 Years	43	22%
3-4 Years	31	15%
More than 4 Years	26	13%
TOTAL	200	100

CHART: 4.1.6 Experience of the respondents

Experience
200 responses



INTERPRETATION

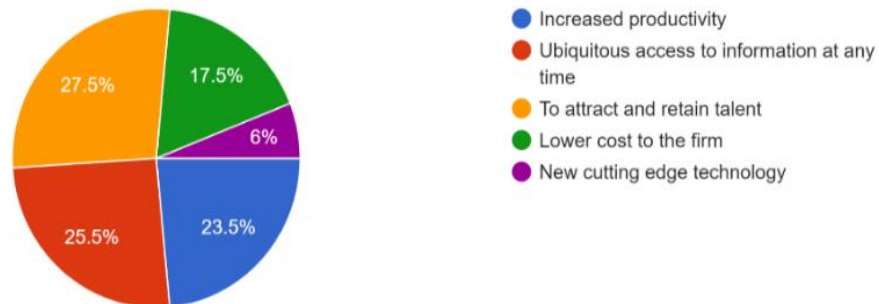
From the above table, it is interpreted that the Experience of the employees. 31% of the respondents are belong to Less than a year experience category, 19% of the respondents are belong to 1-2years experience category, 22% of the respondents are belong to 2-3years experience category, 15% of the respondents are belong to 3-4years experience category and 13% of the respondents are belong to more than 4years experience category.

TABLE: 4.1.7 BYOD Implementation in the Organization

OPINION	NO.OF.RESPONDENTS	PERCENTAGE
Increased productivity	47	23%
Ubiquitous access to information at any time	51	26%
To attract & retain talent	55	28%
Low cost to the firm	35	17%
New cutting edge technology	12	6%
TOTAL	200	100

CHART: 4.1.7 BYOD Implementation in the Organization

How is BYOD implementation resulted in your organization?
200 responses



INTERPRETATION

From the above table, it is interpreted that the BYOD implementation in the Organization of the employees. 23% of the respondents were said Increased productivity, 26% of the respondents were said Ubiquitous access to information at any time, 28% of the respondents were said to attract and retain talent, 17% of the respondents were said Low cost to the firm and 6% of the respondents were said New cutting Technology.

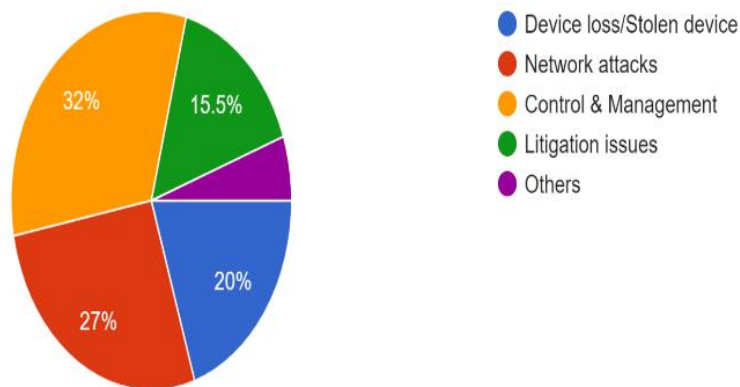
TABLE: 4.1.8 Type of security risks employees face in BYOD

SECURITY RISKS	NO.OF.RESPONDENTS	PERCENTAGE
Device loss/Stolen device	40	20%
Network attacks	54	27%
Control & Management	64	32%
Litigation issues	31	16%
Others	11	5%
TOTAL	200	100

CHART: 4.1.8 Type of security risks employees face in BYOD

What type of security/privacy risks do you face in BYOD implementation?

200 responses



INTERPRETATION

From the above table, it is interpreted that the type of security risks employees faced in BYOD. 20% of the respondents were said Device loss /Stolen device security risk, 27% of the respondents were said Network attacks security risk, 32% of the respondents were said Control & management security risk, 16% of the respondents were said Litigation issues security risk and 5% of the respondents were said Other security risk.

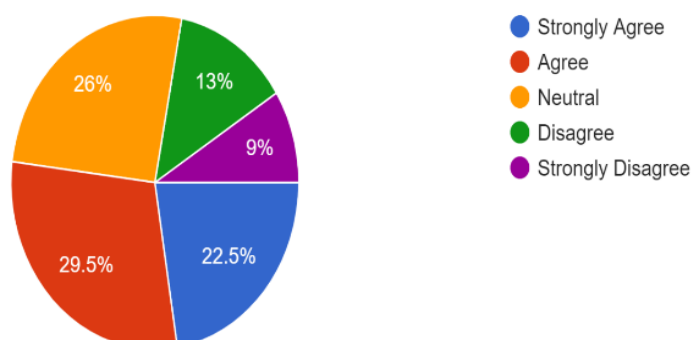
TABLE: 4.1.9 BYOD provides significant move towards safeguarding confidential information

OPINION	NO.OF.RESPONDENTS	PERCENTAGE
Strongly agree	45	22%
Agree	59	30%
Neutral	52	26%
Disagree	26	13%
Strongly Disagree	18	9%
TOTAL	200	100

CHART: 4.1.9 BYOD provides significant move towards safeguarding confidential information

Do you think, BYOD provides significant move towards safeguarding confidential information in the firm?

200 responses



INTERPRETATION

From the above table, it is interpreted that the respondents' opinion about BYOD provides significant move towards safeguarding confidential information. 22% of the respondents were said Strongly agree, 30% of the respondents were said agree, 26% of the respondents were said Neutral, 13% of the respondents were said Disagree and 9% of the respondents were said Strongly Disagree.

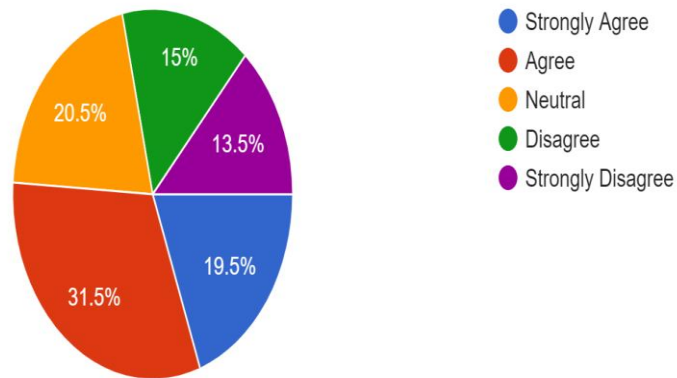
TABLE: 4.1.10 Employees comfortability with BYOD in the organization

OPINION	NO.OF.RESPONDENTS	PERCENTAGE
Strongly agree	39	19%
Agree	63	32%
Neutral	41	21%
Disagree	30	15%
Strongly Disagree	27	13%
TOTAL	200	100

CHART: 4.1.10 Employees comfortability with BYOD in the organization

Are you greatly comfortable with the BYOD implementation in your organization?

200 responses



INTERPRETATION

From the above table, it is interpreted that the respondents' opinion about whether employees comfortable with BYOD in the organization. 19% of the respondents were said Strongly agree, 32% of the respondents were said agree, 21% of the respondents were said Neutral, 15% of the respondents were said Disagree and 13% of the respondents were said Strongly Disagree.

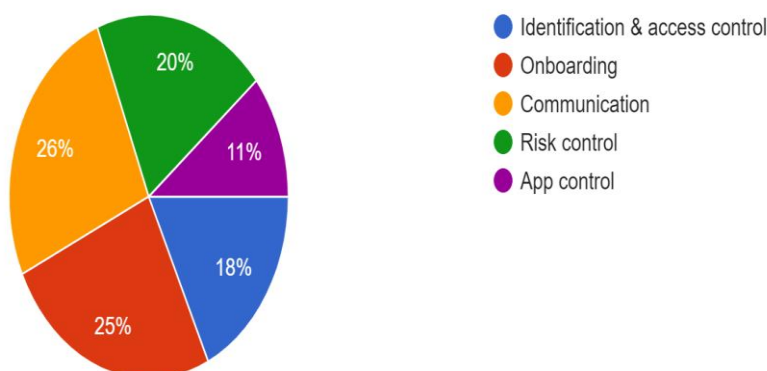
TABLE: 4.1.11 Possible control measures considered for confronting BYOD policies

CONTROL MEASURES	NO.OF.RESPONDENTS	PERCENTAGE
Identification & access control	36	18%
Onboarding	50	25%
Communication	52	26%
Risk control	40	20%
App control	22	11%
TOTAL	200	100

CHART: 4.1.11 Possible control measures considered for confronting BYOD policies

What are the possible control measures should be considered for confronting BYOD policies?

200 responses



INTERPRETATION

From the above table, it is interpreted that the possible control measures considered for confronting BYOD policies. 18% of the respondents were said Identification & access control, 25% of the respondents were said Onboarding control measure, 26% of the respondents were said Communication control measure, 20% of the respondents were said Risk control measure and 11% of the respondents were said App control measure.

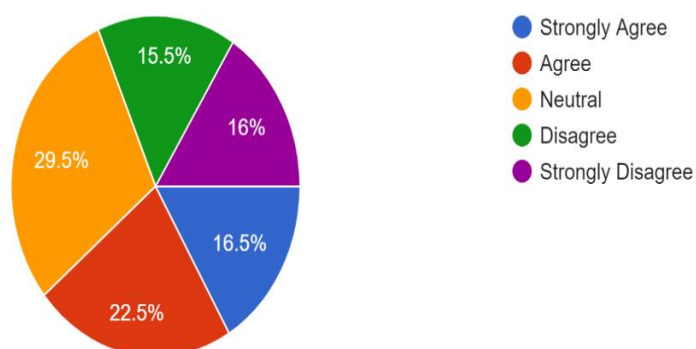
TABLE: 4.1.12 Ineffective management issues resulting in major cause of BYOD security

OPINION	NO.OF.RESPONDENTS	PERCENTAGE
Strongly agree	33	16%
Agree	45	23%
Neutral	59	30%
Disagree	31	15%
Strongly Disagree	32	16%
TOTAL	200	100

CHART: 4.1.12 Ineffective management issues resulting in major cause of BYOD security

Whether "Ineffective management issues results in the major cause of BYOD security in your firm"?

200 responses



INTERPRETATION

From the above table, it is interpreted that the respondents' opinion about the statement whether ineffective management issues results in major cause of BYOD security. 16% of the respondents were said Strongly agree, 23% of the respondents were said agree, 30% of the respondents were said Neutral, 15% of the respondents were said Disagree and 16% of the respondents were said Strongly Disagree.

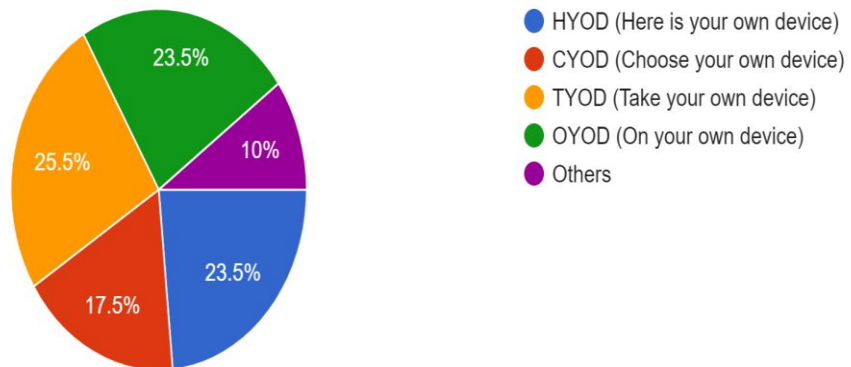
TABLE: 4.1.13 Best mode of approaches in BYOD

APPROACHES	NO.OF.RESPONDENTS	PERCENTAGE
HYOD	47	24%
CYOD	35	17%
TYOD	51	26%
CYOD	47	23%
Others	20	10%
TOTAL	200	100

CHART: 4.1.13 Best mode of approaches in BYOD

Which is the best mode of approaches in BYOD?

200 responses



INTERPRETATION

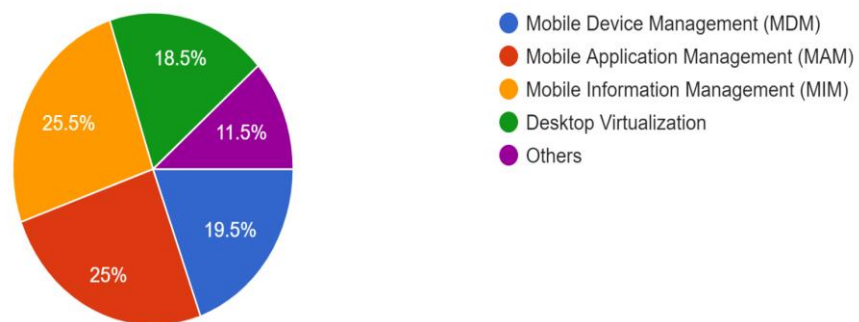
From the above table, it is interpreted that the Best mode of approaches in BYOD. 24% of the respondents were said HYOD mode, 17% of the respondents were said CYOD mode, 26% of the respondents were said TYOD mode, 23% of the respondents were said CYOD mode and 10% of the respondents were said Other modes.

TABLE: 4.1.14 Characteristics of security models employees use for managing BYOD

SECURITY MODELS	NO.OF.RESPONDENTS	PERCENTAGE
Mobile Device Management	39	20%
Mobile Application Management	50	25%
Mobile Information Management	51	26%
Desktop Virtualization	37	18%
Others	23	11%
TOTAL	200	100

CHART: 4.1.14 Characteristics of security models employees use for managing BYOD

Which characteristics of security models you use for managing BYOD?
200 responses



INTERPRETATION

From the above table, it is interpreted that the Characteristics of security models. 20% of the respondents were said Mobile Device Management security model, 25% of the respondents were said Mobile Application Management security model, 26% of the respondents were said Mobile Information Management security model, 18% of the respondents were said Desktop virtualization security model and 11% of the respondents were said Other security models.

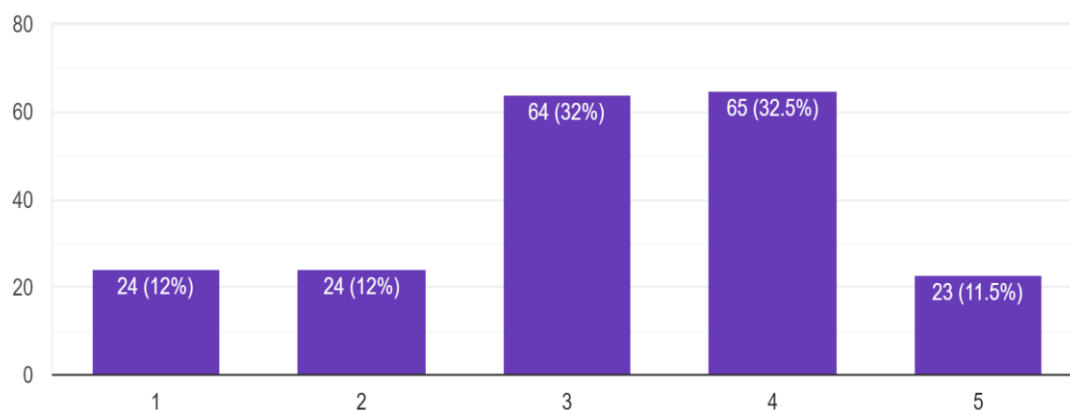
TABLE: 4.1.15 Satisfaction level of BYOD program in the organization

LEVEL OF SATISFACTION	NO.OF.RESPONDENTS	PERCENTAGE
1	24	12%
2	24	12%
3	64	32%
4	65	33%
5	23	11%
TOTAL	200	100

CHART: 4.1.15 Satisfaction level of BYOD program in the organization

Rate your satisfaction level of BYOD program in your organization?

200 responses



INTERPRETATION

From the above table, it is interpreted that employees' satisfaction level of BYOD program in the organization. 12% of the respondents were Highly Dissatisfied, 12% of the respondents were Dissatisfied, 32% of the respondents were neutral, 33% of the respondents were satisfied and 11% of the respondents were Highly Satisfied.

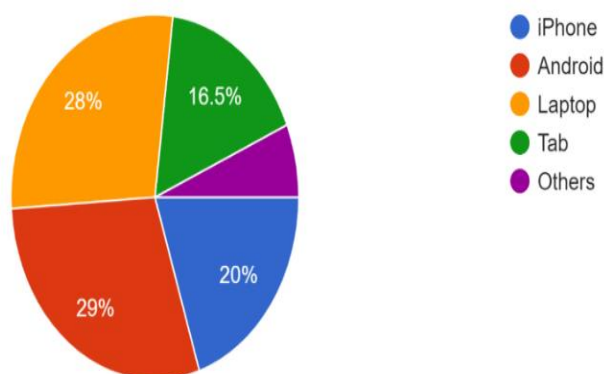
TABLE: 4.1.16 Type of hardware devices employees use under BYOD

HARDWARE DEVICES	NO.OF.RESPONDENTS	PERCENTAGE
iPhone	40	20%
Android	58	29%
Laptop	56	28%
Tab	33	17%
Others	13	6%
TOTAL	200	100

CHART: 4.1.16 Type of hardware devices employees use under BYOD

What type of hardware devices you are using under BYOD policy in your organization?

200 responses



INTERPRETATION

From the above table, it is interpreted that the type of hardware devices employees' used under BYOD policy. 20% of the respondents were said iPhone, 29% of the respondents were said Android, 28% of the respondents were said Laptop, 17% of the respondents were said Tab and 6% of the respondents were said Other devices.

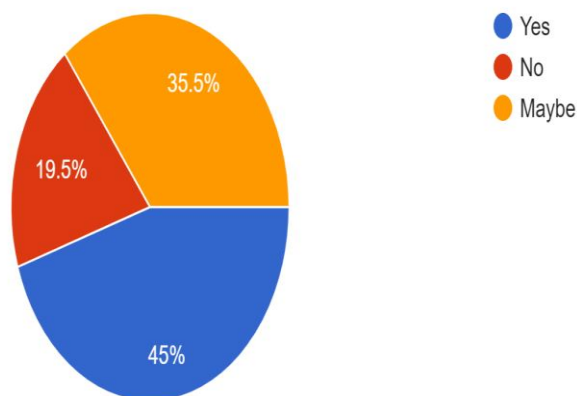
TABLE: 4.1.17 Organization have proper infrastructure in place to support BYOD

OPINION	NO.OF.RESPONDENTS	PERCENTAGE
Yes	90	45%
No	39	19%
May be	71	36%
TOTAL	200	100

CHART: 4.1.17 Organization have proper infrastructure in place to support BYOD

Does your organization have the proper infrastructure in place to support BYOD?

200 responses



INTERPRETATION

From the above table, it is interpreted that the organization have proper infrastructure in place to support BYOD. 45% of the respondents were said Yes Opinion, 19% of the respondents were said No opinion and 36% of the respondents were said Maybe opinion.

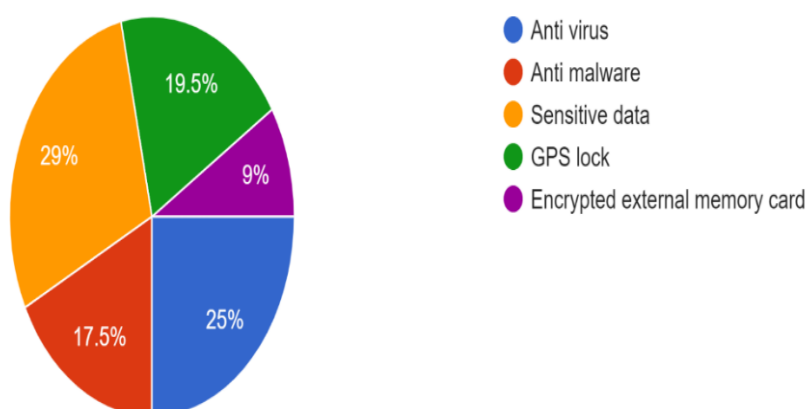
TABLE: 4.1.18 Basic control methods employees using for BYOD environment

CONTROL METHODS	NO.OF.RESPONDENTS	PERCENTAGE
Anti virus	50	25%
Anti Malware	35	17%
Sensitive data	58	29%
GPS lock	39	20%
External memory card	18	9%
TOTAL	200	100

CHART: 4.1.18 Basic control methods employees using for BYOD environment

Which basic control methods you are using in your firm for BYOD environment?

200 responses



INTERPRETATION

From the above table, it is interpreted that the Basic control methods employees' using in firm for BYOD environment. 25% of the respondents were said Anti virus method, 17% of the respondents were said Anti malware method, 29% of the respondents were said Sensitive data method, 20% of the respondents were said GPS lock method and 9% of the respondents were said Other methods.

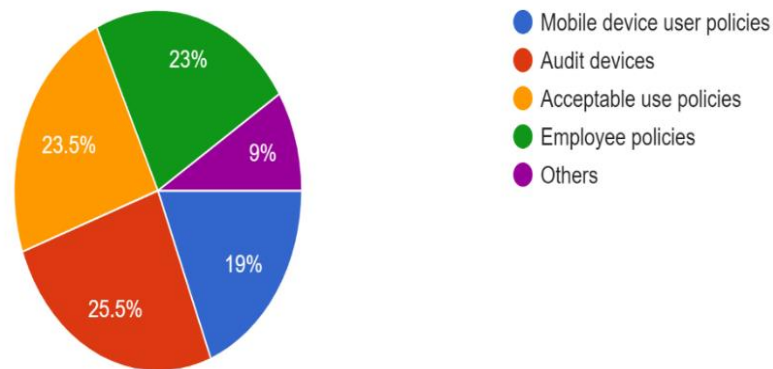
TABLE: 4.1.19 BYOD policy that the Organization follows

POLICY	NO.OF.RESPONDENTS	PERCENTAGE
Mobile device user policies	38	19%
Audit devices	51	26%
Acceptable use policies	47	23%
Employer policies	46	23%
Others	18	9%
TOTAL	200	100

CHART: 4.1.19 BYOD policy that the Organization follows

Which BYOD policy does your organization follows?

200 responses



INTERPRETATION

From the above table, it is interpreted that what BYOD policy does the organization follows. 19% of the respondents were said Mobile device user policies, 26% of the respondents were said Audit devices, 23% of the respondents were said Acceptable use policies, 23% of the respondents were said employee policies and 9% of the respondents were said other policies.

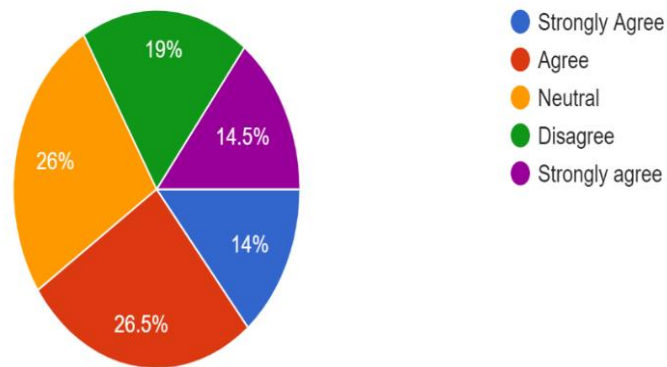
TABLE: 4.1.20 BYOD management & stipends cost more than company devices

OPINION	NO.OF.RESPONDENTS	PERCENTAGE
Strongly agree	28	14%
Agree	53	27%
Neutral	52	26%
Disagree	38	19%
Strongly Disagree	29	14%
TOTAL	200	100

CHART: 4.1.20 BYOD management & stipends cost more than company devices

Do you agree "BYOD management and stipends cost more than just providing company devices"?

200 responses



INTERPRETATION

From the above table, it is interpreted that the respondents' opinion about the statement whether BYOD management & stipends cost more than just providing company devices. 14% of the respondents were said Strongly agree, 27% of the respondents were said agree, 26% of the respondents were said Neutral, 19% of the respondents were said Disagree and 14% of the respondents were said Strongly Disagree.

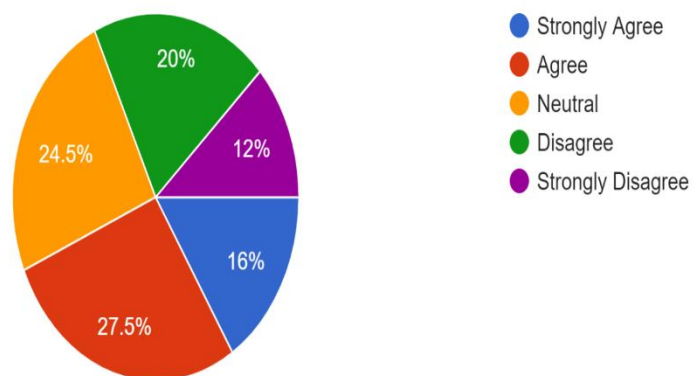
TABLE: 4.1.21 BYOD provides right balance between productivity & security

OPINION	NO.OF.RESPONDENTS	PERCENTAGE
Strongly agree	32	16%
Agree	55	28%
Neutral	49	24%
Disagree	40	20%
Strongly Disagree	24	12%
TOTAL	200	100

CHART: 4.1.21 BYOD provides right balance between productivity & security

Whether BYOD policy in your firm provides right balance between productivity and security?

200 responses



INTERPRETATION

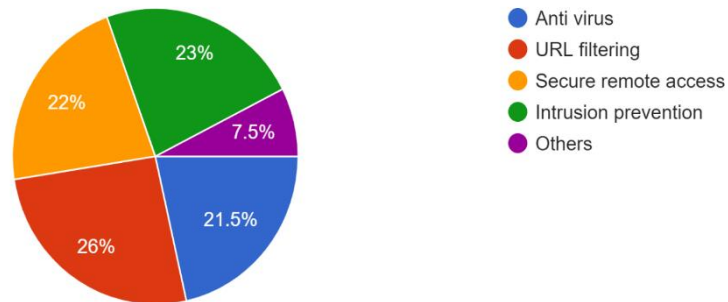
From the above table, it is interpreted that the BYOD provides right balance between productivity & security. 16% of the respondents were said Strongly agree, 28% of the respondents were said agree, 24% of the respondents were said Neutral, 20% of the respondents were said Disagree and 12% of the respondents were said Strongly Disagree.

TABLE: 4.1.22 Established security procedures to handle BYOD in the organization

SECURITY PROCEDURES	NO.OF.RESPONDENTS	PERCENTAGE
Anti virus	43	22%
URL filtering	52	26%
Secure remote access	44	22%
Intrusion prevention	46	23%
Others	15	7%
TOTAL	200	100

CHART: 4.1.22 Established security procedures to handle BYOD in the organization

What are the established security procedures to handle BYOD in your organization?
200 responses



INTERPRETATION

From the above table, it is interpreted that established security procedures to handle BYOD in organization. 22% of the respondents were said Anti virus security procedure, 26% of the respondents were said URL filtering security procedure, 22% of the respondents were said secure remote access security procedure, 23% of the respondents were said Intrusion prevention security procedure and 7% of the respondents were said Other security procedures.

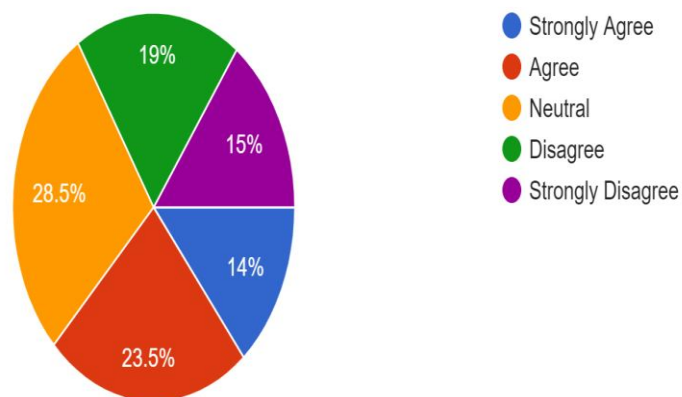
TABLE: 4.1.23 BYOD program is right fit for the working organization

OPINION	NO.OF.RESPONDENTS	PERCENTAGE
Strongly agree	28	14%
Agree	47	23%
Neutral	57	29%
Disagree	38	19%
Strongly Disagree	30	15%
TOTAL	200	100

CHART: 4.1.23 BYOD program is right fit for the working organization

Do you think, BYOD program is the right fit for your working organization?

200 responses



INTERPRETATION

From the above table, it is interpreted that the BYOD program is right fit for the working organization. 14% of the respondents were said Strongly agree, 23% of the respondents were said agree, 29% of the respondents were said Neutral, 19% of the respondents were said Disagree and 15% of the respondents were said Strongly Disagree.

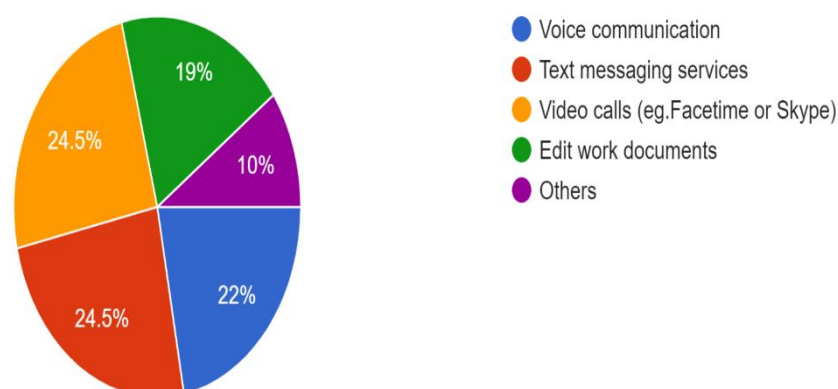
TABLE: 4.1.24 Table indicating work tasks in BYOD

WORK TASKS	NO.OF.RESPONDENTS	PERCENTAGE
Voice communication	44	22%
Text messaging services	49	25%
Video calls (eg. Skype or Facetime)	49	24%
Edit work documents	38	19%
Others	20	10%
TOTAL	200	100

CHART: 4.1.24 Chart indicating work tasks in BYOD

What work task would you find useful to do on your own device in BYOD?

200 responses



INTERPRETATION

From the above table, it is interpreted that the work tasks employees' found useful in BYOD. 22% of the respondents were said Voice communication, 25% of the respondents were said Text messaging services, 24% of the respondents were said Video calls, 19% of the respondents were said Edit work documents and 10% of the respondents were said Other work tasks.

4.2 ANOVA

AIM: To find out the relationship between experience and the work tasks assigned to the employees under BYOD policy.

- **Ho:** There is no significant relationship between various department and positive influence of BYOD in the firm.
- **H1:** There is a significant relationship between various department and positive influence of BYOD in the firm.

ANOVA

Department

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2.296	4	.574	.305	.874
Within Groups	366.424	195	1.879		
Total	368.720	199			

TABLE: 4.2.1 Anova analysis

INTERPRETATION

By using anova for finding the relationship between the Department & BYOD policy in the firm provides right balance between productivity and security, that the p value is 0.874 which is greater than the significant level (0.05). Hence, Ho is accepted and H1 gets rejected.

ANOVA

Experience

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	18.459	4	4.615	2.423	.090
Within Groups	371.336	195	1.904		
Total	389.795	199			

TABLE: 4.2.2 Anova analysis

INTERPRETATION

By using anova for finding the relationship between the Experience & work task that employee found useful to do on own device under BYOD, that the p value is 0.090 which is higher than the significant level (0.05). Hence, Ho is accepted and H1 gets rejected.

4.3 CORRELATION

AIM: To find out the relationship between experience and the work tasks assigned to the employees under BYOD policy.

- **Ho:** There is no significant relationship between experience and work tasks assigned to the employees under BYOD policy.
- **H1:** There is a significant relationship between experience and work tasks assigned to the employees under BYOD policy.

Correlations

		Whether BYOD policy in your firm provides right balance between productivity and security?	Department
Whether BYOD policy in your firm provides right balance between productivity and security?	Pearson Correlation	1	-.046
	Sig. (2-tailed)		.521
	N	200	200
Department	Pearson Correlation	-.046	1
	Sig. (2-tailed)	.521	
	N	200	200

TABLE: 4.3.1 Table indicating correlation analysis

INTERPRETATION

By using the Correlation for finding the relationship between, Department of the employees and BYOD policy in the firm provides right balance between productivity & security that, we found that there is a Negative correlation underlies between both the factors with the value of 0.01 level of significance and also found that weak relationship (-0.046) found between each variable.

Correlations

		What work task would you find useful to do on your own device in BYOD?	Experience
What work task would you find useful to do on your own device in BYOD?	Pearson	1	.187**
	Correlation		
	Sig. (2-tailed)		.008
	N	200	200
Experience	Pearson	.187**	1
	Correlation		
	Sig. (2-tailed)	.008	
	N	200	200

** . Correlation is significant at the 0.01 level (2-tailed).

TABLE: 4.3.2 Table indicating correlation analysis

INTERFERENCE

By using the Correlation for finding the relationship between, experience of the employees and work task that employee found useful to do on own device under BYOD, we found that there is a positive correlation underlies between both the factors with the value of 0.01 level of significance and also found that strong relationship (0.187) found between each variable.

CHAPTER 5

FINDINGS, SUGGESTIONS AND CONCLUSION

5.1 FINDINGS

- Majority 63% of the respondents are male.
- 40% of the respondents belong to the age group of below 25 Category.
- 58% of the respondents were married.
- 48% of the respondents belongs to UG educational qualification.
- 26% of the respondents belongs to Accounts department.
- 31% of the respondents had less than a year experience.
- 28% of the respondents said that BYOD implementation resulted in to attract & retain talent.
- 32% of the respondents said control & management type of security risk exist in BYOD implementation.
- 30% of the respondents said agreed that BYOD provides significant move towards safeguarding confidential information in the firm.
- 32% of the respondents agreed that they were comfortable with the BYOD implementation in your organization.
- 26% of the respondents said that communication is the possible control measure for BYOD policy.
- 30% of the respondents were neutral that ineffective management issues results in the major cause of BYOD security in the firm.
- 26% of the respondents said that TYOD is the best mode of approaches in BYOD.
- 26% of the respondents using Mobile Information Management characteristics of security models for managing BYOD.
- 33% of the respondents were satisfied with BYOD policy.
- 29% of the respondents were using android under BYOD policy in the organization.
- 45% of the respondents said that proper infrastructure exists in place to support BYOD.
- 29% of the respondents said that sensitive data control method
- 26% of the respondents were following audit devices BYOD policy.

- 27% of the respondents agreed that BYOD management & stipends cost more than just providing devices.
- 28% of the respondents agreed that the BYOD provides right balance between productivity and security.
- 26% of the employees said that URL filtering is used as the established security procedure to handle BYOD in the organization.
- 29% of the respondents neutrally said that the BYOD program is the right fit for the working organization.
- 25% of the respondents equally said that text messaging services and video calls were the work tasks they found useful to do on their own device in BYOD.
- By using anova for finding the relationship between the Department & BYOD policy in the firm provides right balance between productivity and security, that the p value is 0.874 which is greater than the significant level(0.05). Hence, Ho is accepted and H1 gets rejected.
- By using anova for finding the relationship between the Experience & work task that employee found useful to do on own device under BYOD, that the p value is 0.090 which is higher than the significant level (0.05). Hence, Ho is accepted and H1 gets rejected.
- By using the Correlation for finding the relationship between, Department of the employees and BYOD policy in the firm provides right balance between productivity & security that, we found that there is a Negative correlation underlies between both the factors with the value of 0.01 level of significance and also found that weak relationship (-0.046) found between each variable.
- By using the Correlation for finding the relationship between, experience of the employees and work task that employee found useful to do on own device under BYOD, we found that there is a positive correlation underlies between both the factors with the value of 0.01 level of significance and also found that strong relationship (0.187) found between each variable.

5.2 SUGGESTIONS & RECOMMENDATIONS

- To create a holistic and effective BYOD framework that ensures the security & privacy objectives of confidentiality, integrity, BYOD must

elucidate the fundamental policies & standards of communication.

- Adopting and implementing an effective BYOD program is a responsibility that is not only restricted to IT network administrators but also it is a responsibility that should be undertaken by the firm and its employee in general.
- Intrinsically, an all-inclusive BYOD policy is required to ensure that the BYOD is not only efficacious but likewise secure. Here are some recommendations to aid organizations with their BYOD adoption.
- Policy considerations like Employee training on privacy awareness, Regular policy update encourages BYOD adoption in the firm.
- Corporate firms could also employ Virtual Private Network (VPN) to permit employees that remotely access IT infrastructure and to apply caution to avoid network attacks.

5.3. CONCLUSION

BYOD has become a good strategy that companies use due to their great benefits; companies like CISCO and others create technical solutions and implement policies to help mitigate the risks. BYOD policy security and privacy potential problems assessment is a significant move towards safeguarding the effective BYOD adoption, implementation, and management of confidential information in its framework. This work proffers unambiguous understanding of BYOD security risks and threats to adopters and users by identification and classification of possible list of threats/vulnerabilities of BYOD adoption that should be applied by firms and users to mitigate BYOD risks using a layered approach. According to the, notwithstanding that BYOD is an influential idea with the vast potential to strengthen productivity and effectiveness, organizations should adopt policies, procedures and standards that have the most fitting technical controls to avert organizational and employee's loss of confidential information. Technically, it is expected that the contribution of this research by implementation will be advantageous to employees and firms that use BYOD policies in the course of accomplishing its organizational goals. The use of BYOD is becoming widespread, and due to the security risks organizations should also have and enforce BYOD policies. One of the most important best practices is to balance the flexibility provided by BYOD with necessary security policies that do not negate the end user's abilities to perform their jobs.

REFERENCES

ARTICLES

- Ackerman, E. (2013). The bring-your-own-device dilemma: Employees and businesses seek to balance privacy and security. *IEEE Spectrum*, 50(8), 22–22. <http://dx.doi.org/10.1109/MSPEC.2013.6565553>
- Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, 42, 56–65. <http://dx.doi.org/10.1016/j.cose.2014.01.005>
- Armando, A., Costa, G., Verderame, L., & Merlo, A. (2014). Securing the “bring your own device” paradigm. *Computer*, 47(6), 48–56. <http://dx.doi.org/10.1109/MC.2014.164>
- Center for Public Issues Education. (2014.). Evaluating information sources. Retrieved from <http://ce.uoregon.edu/aim/Capstone1Perm/evaluateinfo.pdf>
- Chang, J. M., Ho, P.-C., & Chang, T.-C. (2014). Securing BYOD. *IT Professional*, 16(5), 9–11. <http://dx.doi.org/10.1109/MITP.2014.76>
considerations. *IT Professional*, 14(5), 53–55. <http://dx.doi.org/10.1109/MITP.2012.93>
- Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, 28(1), 209–226. <http://dx.doi.org/10.2308/isis-50704>
- Disterer, G., & Kleiner, C. (2013). BYOD Bring your own device. *Procedia Technology*, 9, 43– 53. <http://dx.doi.org/10.1016/j.protcy.2013.12.005>
- Earley, S., Harmon, R., Lee, M. R., & Mithas, S. (2014). From BYOD to BYOA, Phishing, and Botnets. *IT Professional*, 16(5), 16–18. <http://dx.doi.org/10.1109/MITP.2014.69>
- Fiorenza, P. (2013). Mobile technology forces study of bring your own device. *Public Manager*, 42(1), 12-14.

- Ghosh, A., Gajar, P. K., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science*, 4(4), 62–70
- Hayes, B., & Kotwica, K. (2013). Bring your own device (BYOD) to work:
- Jaramillo, D., Katz, N., Bodin, B., Tworek, W., Smart, R., & Cook, T. (2013). Cooperative solutions for bring your own device (BYOD). *IBM Journal of Research and Development*, 57(6): 5.
- Johnson, K. & Filkins, B.L. (2012). SANS mobility/BYOD security survey. Retrieved from http://www.sans.org/reading_room/analysts_program/mobility-security-survey.pdf
- Li, Q., & Clark, G. (2013). Mobile security: A look ahead. *IEEE Security*
- Marjanovic, Z. (2013). Effectiveness of security controls in BYOD environments. The University of Melbourne, Australia. Retrieved from <http://hdl.handle.net/11343/33346>
- Marjanovic, Z. (2013). Effectiveness of security controls in BYOD environments. The University of Melbourne, Australia. Retrieved from <http://hdl.handle.net/11343/33346>
- Mitrovic, Z., Veljkovic, I., Whyte, G., & Thompson, K. (2014). Introducing BYOD in an organisation: The risk and customer services viewpoints. Paper presented at The 1st Namibia Customer Service Awards & Conference, in Windhoek, Namibia. Retrieved from <http://ir.polytechnic.edu.na/handle/10628/522>
- Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, 2012(12), 5–8.
- Rivera, D., George, G., Peter, P., Muralidharan, S., & Khanum, S. (2013). Analysis of security controls for BYOD (bring your own device). The University of Melbourne, Australia. Retrieved from <http://hdl.handle.net/11343/33338>
- Scardilli, B. (2014). BYOD or COPE: The best mobile strategy for the workplace. *Information Today*, 31(2). Retrieved from <https://www.questia.com/magazine/1G1-363515159/byod-or-cope-the-best-mobile-strategy-for-the-workplace>

- Thomson, G. (2012). BYOD: Enabling the chaos. Network Security, 2012(2), 5–8.
- Tokuyoshi, B. (2013). The security implications of BYOD. Network Security, 2013(4), 12–13.
- Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD. Procedia Computer Science, 50, 511–516.
<http://dx.doi.org/10.1016/j.procs.2015.04.023>
- Waterfill, M. R., & Dilworth, C. A. (2014). BYOD: Where the employee and the enterprise intersect. Employee Relations Law Journal, 40(2), 26–36
- Webroot. (2014). Fixing the disconnect between employer and employee for BYOD (bring your own device). Retrieved from <http://www.webroot.com/shared/pdf/WebrootBYODSecurityReport2014.pdf>.

GENERAL REFERENCE FROM BOOKS

- Bennet, L. & TUCKER, H. A Handbook of Bring Your Own Device. ITNOW, 54(1).
- CHANG, J.M., HO, P & CHANG, a book about T. Securing BYOD published on 2014.
- HAYES, B. E. & KOTWICA K. Bring your own device (BYOD) to work.

WEBSITES

www.byodpolicy.com

ANNEXURE I
QUESTIONNAIRE
A STUDY ON EMPLOYEE PERCEPTION TOWARDS BYOD AT
FABSYS TECHNOLOGIES PRIVATE LIMITED

Dear Sir /Madam,

I am Kanimozhi M doing a project in Fabsys Technologies Private Limited conducting a survey on “A STUDY ON EMPLOYEE PERCEPTION TOWARDS BYOD AT FABSYS TECHNOLOGIES PRIVATE LIMITED”. This Questionnaire is only for academic purpose and would be kept confidential.

Personal Information

1. Name of the Employee:
2. Gender of the Employee:
 - a) Male
 - b) Female
3. Age (in Years) of the Employee:
 - a) Below 25
 - b) 26 to 30
 - c) 31 to 35
 - d) 36 to 40
 - e) Above 40
4. Marital Status of the Employee:
 - a) Married
 - b) Unmarried
5. Educational Qualification of the Employee:
 - a) School
 - b) Diploma
 - c) UG
 - d) PG
 - e) Others
6. Department of the Employee:
 - a) HR
 - b) Accounting
 - c) Service

- d) Marketing
- e) Others

7.Experience of the Employee:

- a) Less than a year
- b) 1-2 years
- c) 2-3 years
- d) 3-4 years
- e) More than 4 years

8.How is BYOD implementation resulted in your organization?

- a) Increased Productivity
- b) Ubiquitous access to information at any time
- c) To attract and retain talent
- d) Lower cost to the firm
- e) New cutting edge technology

9.What type of security/privacy risks do you face in BYOD implementation?

- a) Device loss/Stolen device
- b) Network attacks
- c) Control & management
- d) Litigation issues
- e) Others

10.Do you think, BYOD provides significant move towards safeguarding confidential information in the firm?

- a) Strongly Agree
- b) Agree
- c) Neutral
- d) Disagree
- e) Strongly Disagree

11.Are you greatly comfortable with the BYOD policy implementation in your company?

- a) Strongly Agree
- b) Agree
- c) Neutral
- d) Disagree
- e) Strongly Disagree

12.What are the possible control measures should be considered for confronting BYOD policies?

- a) Identification & access control
- b) Onboarding
- c) Communication
- d) Risk control
- e) App Control

13. Whether “Ineffective management issues results in the major cause of BYOD security in your firm”?

- a) Strongly Agree
- b) Agree
- c) Neutral
- d) Disagree
- e) Strongly Disagree

14.Which is the best mode of approaches in BYOD?

- a) HYOD (Here is your own device)
- b) CYOD (Choose your own device)
- c) ONOD (On your own device)
- d) TYOD (Take your own device)
- e) Others

15.Which characteristics of security models you use for managing BYOD?

- a) Mobile Device Management
- b) Mobile Application Management
- c) Mobile Information Management
- d) Desktop Virtualization
- e) Others

16.Rate your satisfaction level of BYOD program in your organization?

1	2	3	4	5
DISLIKE	(LIKERT SCALE)			LIKE

17.What type of hardware devices you are using under BYOD policy in your organization?

- a) iPhone
- b) Android
- c) Laptop

- d) Tab
- e) Others

18. Does your organization have the proper infrastructure in place to support BYOD?

- a) Yes
- b) No
- c) Maybe

19. Which basic control methods you are using in your firm for BYOD environment?

- a) Anti-virus
- b) Anti malware
- c) GPS lock
- d) Sensitive data
- e) External Memory card

20. Which BYOD policy does your organization follows?

- a) Mobile devices user policies
- b) Audit devices
- c) Acceptable use policies
- d) Employee policies
- e) Others

21. Do you agree, "BYOD management and stipends cost more than just providing company devices"?

- a) Strongly Agree
- b) Agree
- c) Neutral
- d) Disagree
- e) Strongly Disagree

22. Whether BYOD policy in your firm provides right balance between productivity and security?

- a) Strongly Agree
- b) Agree
- c) Neutral
- d) Disagree
- e) Strongly Disagree

23. What are the established security procedures to handle BYOD in your organization?

- a) Anti-virus
- b) URL filtering
- c) Secure remote access
- d) Intrusion prevention
- e) Others

24. Do you think; BYOD program is the right fit for your working organization?

- a) Strongly Agree
- b) Agree
- c) Neutral
- d) Disagree
- e) Strongly Disagree

25. What work tasks would you find useful to do on your own device in BYOD?

- a) Voice communication
- b) Text messaging services
- c) Video calls (eg.Facetime or Skype)
- d) Edit work documents
- e) Others

ANNEXURE II RESEARCH ARTICLE

A STUDY ON THE EMPLOYEE PERCEPTION TOWARDS BYOD AT FABSYS TECHNOLOGIES PRIVATE LIMITED

DR. A.S. PRINCY¹ & M. KANIMOZHI²

¹*Assistant Professor, School of Management Studies, Sathyabama Institute of Science and Technology,
Chennai, Tamil Nadu, India*

²*MBA Student, School of Management Studies, Sathyabama Institute of Science and Technology,
Chennai, Tamil Nadu, India*

ABSTRACT:

This project titled “A Study on employee perception towards BYOD at Fabsys Technologies Private Limited” aims at understanding the overall effectiveness of using this concept in the corporate world. Bring Your Own Device refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications. This study has a scope to get a better Policy for BYOD implementation in IT Environment. This study enables us to frame an action plan to overcome the security issues and also to show improvement in IT Business Cycle. Multiple choice questions have been chosen to collect the responses from 200 companies. Numerous new findings have been derived from this research has helped to provide few suggestions to the company to improve the employee perception towards BYOD.

KEYWORDS:

BYOD, Security issues, IT environment, employees, perception, workplace, mobile devices.

INTRODUCTION:

Bring Your Own Device refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications. The term is also used to describe the same practice applied to students using personally owned devices in education settings. BYOD is making significant inroads in the business world, with about 75% of employees in high growth markets such as Brazil and Russia and 44% in developed markets already using their own technology at work. In most cases, business simply can't block the trend. Some believe that BYOD may help employees be more productive. Others say it increases employee morale and convenience by using their own devices and makes the company look like a flexible and attractive employer. Many feel that BYOD can even be a means to attract new hires, pointing to a survey that indicates 44% of job seekers view an organization more positively if it supports their device.

OBJECTIVES:

- To study the need for implementing BYOD in Fabsys Technologies Private Limited.
- To assess the various security related issues associated with BYOD.
- To know the efficiency of the BYOD.

SCOPE OF THE STUDY:

- Increase in Productivity and thereby firms profit
- Research enables the company to evaluate the operating efficiency of the BYOD
- New Policy (BYOD) Implementation in IT Environment.
- Strategy for implementation of BYOD by Fabsys Technologies Pvt Ltd in the future
- Action plan to overcome the security issues.
- Improvement in IT Business Cycle.

NEED FOR THE STUDY:

Mobility is one of the hottest trends in technology, with cell phones, tablets, and other mobile devices being brought to the workplace in ever-increasing numbers. Known as "bring your own device" (BYOD), this change is clearly here to stay. As more employees bring their own mobile devices to work, companies must assess the security risks and costs. By doing nothing, company security is at risk as employee's access email and other potentially proprietary data on their mobile devices. With a policy in place, access to data is controlled, and productivity can be extended to these devices.

Through this research, a thorough analysis of the BYOD implementation has to be made to promote the benefits of BYOD to Fabsys. This study will enlighten the readers about the various advantages and the measures to be taken for successful implementation of BYOD at Fabsys.

REVIEW OF LITERATURE:

K. G. Gökçe & O. Dogerlioglu (2023). This study reviews advantages and disadvantages of using "personally owned device" in the workplace. The research looks at the field from two different perspectives: Employees and managers. Manager perspective is enlightened with the help of interviews. Interview data and literature review provided the basis for the survey instrument which served to learn employee perspective.

Ackerman, (2022) Employees and employers have fundamental disagreements on the restrictions that should be placed on personal devices used for work purposes. Employers want to control the devices that connect to their networks, while many employees refuse to allow others privileged access to their personal devices such as admin, root, remote-wipe, or find my iPhone.

U. Vignesh, S. Asha (2021) conducted a survey about Modifying Security Policies Towards BYOD in the IT Consumerization phase, the organizations permit their employees to bring their personally owned device to workplace. This is achieved through enforcing policy or agreement - Bring Your Own Device. The BYOD policies adopted in numerous organizations are vague and generally immature. The prevailing security policies in BYOD are no more supportive for mobile devices like smartphones, tablets and laptops. The security policies must be modified to suit these devices. To mitigate this downside, 3-tier enhanced policy architecture is proposed which specifies the policies to be followed by the device, applications and organizations.

Bashayer Alotaibi, Haya Almagwashi (2018) tells about the survey regarding A Review of BYOD Security Challenges, Solutions and Policy Best Practices 2018 Recently, many employees' own smartphones and tablets; where they use these devices in the workplace either for personal use or to perform functional tasks. Perhaps this considered as the main motivation for numerous organization to pay attention to 'bring your own device' business trend; which is related to the use of personal devices for business purposes. For an organization, this brings some opportunities and security risks. The establish of BYOD policies always be a tough task, as an organization needs to avoid security risks and increase employee productivity. However, the associated security risks with BYOD policy can be managed by developing an effective security policy and adopt some technical security control and procedures. This research paper covers the review of current BYOD security challenges and issues, security solutions and policy best practices in organizational perspective. Moreover, a comprehensive security policy model presented and discussed.

Sara Ali, Muhammad Nauman Qureshi & Abdul Ghafoor Abbasi (2015). This study tells about The trend of adapting BYOD or "Bring Your Own Device" concept in enterprise environment is increasing due to mutual benefits that the company and employees get. Organizations get benefit of increased productivity and reduced IT expenditure whereas the employees are able to use the mobile device which is comfortable and convenient for them. However, BYOD deployment brings serious security and privacy concerns. Critical information of organizations can be leaked if proper measures are not taken to secure BYOD devices. Moreover, if due to BYOD model, customer's data gets lost or compromised then the company's reputation and trust relationship might get damaged. This paper analyzes threats associated with BYOD, presents security requirements and provides classification of BYOD security models as discussed in literature till date. Based on the identified gaps, it further provides a comprehensive design which meets the basic security requirements for BYOD paradigm. The proposed framework does not require modification to the underlying kernel and allows the IT administrator to remotely manage and control BYOD devices.

RESEARCH DESIGN

The study is descriptive in nature. This research is basically fact finding with adequate interpretation using simple analysis of data and by developing thinking and elaborating of patterns and obtaining tentative generalizations as

hypothesis.

SOURCES OF DATA:

- **Primary Data** – Questionnaire given to 150 respondents
- **Secondary Data** – Websites, Published reports & Review of literature from published articles.

HYPOTHESIS:

- **HYPOTHESIS -1**

H₀: There is no significant relationship between various department and positive influence of BYOD in the firm.

H₁: There is a significant relationship between various department and positive influence of BYOD in the firm.

- **HYPOTHESIS-2**

H₀: There is no significant relationship between experience and work tasks assigned to the employees under BYOD policy.

H₁: There is a significant relationship between experience and work tasks assigned to the employees under BYOD policy.

PERCENTAGE ANALYSIS:

Research questions are always answered with a descriptive statistic generally either percentage or mean. Percentage is appropriate when it is important to know how many of the participants gave a particular answer. Generally, percentage is reported when the responses have discrete categories.

Particulars	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
Right Fit	14	23	29	19	15
Right balance between productivity & security	16	28	24	20	12
Ineffective management issues	16	23	30	15	16
Safeguarding confidential information	22	30	26	13	9
Factor of comfortability	19	32	21	15	13

INTERPRETATION:

- Table it is interpreted that the number of respondents were 15% is strongly disagree, 19% is disagree, 29 is Neutral, 23% is agree & 14% is strongly agree.
- Table it is interpreted that the number of respondents were 12% is strongly disagree, 20% is disagree, 24 is Neutral, 28% is agree & 16% is strongly agree.
- Table it is interpreted that the number of respondents were 16% is strongly disagree, 15% is disagree, 30 is Neutral, 23% is agree & 16% is strongly agree.
- Table it is interpreted that the number of respondents were 9% is strongly disagree, 13% is disagree, 26 is Neutral, 30% is agree & 22% is strongly agree.
- Table it is interpreted that the number of respondents were 13% is strongly disagree, 15% is disagree, 21 is Neutral, 32% is agree & 19% is strongly agree.

INTERFERENCE:

- Majority 29% of the respondents neutral with the BYOD is right fit for the organization.
- Majority 28% of the respondents agree that BYOD provides right balance between productivity & security.
- Majority 30 of the respondents were neutral with the ineffective management issues.
- Majority 30% of the respondents agree that BYOD safeguarding confidential information.
- Majority 32% of the respondents agree with the BYOD factor of comfortability.

ANOVA

Department

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2.296	4	.574	.305	.874
Within Groups	366.424	195	1.879		
Total	368.720	199			

INTERPRETATION:

By using anova for finding the relationship between the Department & BYOD policy in the firm provides right balance between productivity and security, that the p value is 0.874 which is greater than the significant level (0.05). Hence, Ho is accepted and H1 gets rejected.

Experience

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	18.459	4	4.615	2.423	.090
Within Groups	371.336	195	1.904		
Total	389.795	199			

INTERPRETATION:

By using anova for finding the relationship between the Experience & work task that employee found useful to do on own device under BYOD, that the p value is 0.090 which is higher than the significant level (0.05). Hence, Ho is accepted and H1 gets rejected.

CORRELATION

		Whether BYOD policy in your firm provides right balance between productivity and security?	Department
Whether BYOD policy in your firm provides right balance between productivity and security?	Pearson Correlation	1	-.046
	Sig. (2-tailed)		.521
	N	200	200
Department	Pearson Correlation	-.046	1
	Sig. (2-tailed)	.521	
	N	200	200

INTERPRETATION:

By using the Correlation for finding the relationship between, Department of the employees and BYOD policy in the firm provides right balance between productivity & security that, we found that there is a Negative correlation underlies between both the factors with the value of 0.01 level of significance and also found that weak relationship (-0.046) found between each variable.

		What work task would you find useful to do on your own device in BYOD?	Experience
What work task would you find useful to do on your own device in BYOD?	Pearson Correlation	1	.187**
	Sig. (2-tailed)		.008
	N	200	200
Experience	Pearson Correlation	.187**	1
	Sig. (2-tailed)	.008	
	N	200	200

INTERPRETATION:

By using the Correlation for finding the relationship between, experience of the employees and work task that employee found useful to do on own device under BYOD, we found that there is a positive correlation underlies between both the factors with the value of 0.01 level of significance and also found that strong relationship (0.187) found between each variable.

FINDINGS:

- Majority 63% of the respondents are male.
- 40% of the respondents belong to the age group of below 25 Category.
- 58% of the respondents were married.
- 48% of the respondents belongs to UG educational qualification.
- 26% of the respondents belongs to Accounts department.
- 31% of the respondents had less than a year experience.
- 28% of the respondents said that BYOD implementation resulted in to attract & retain talent.
- 32% of the respondents said control & management type of security risk exist in BYOD implementation.
- 30% of the respondents said agreed that BYOD provides significant move towards safeguarding confidential information in the firm.
- 32% of the respondents agreed that they were comfortable with the BYOD implementation in your organization.
- 26% of the respondents said that communication is the possible control measure for BYOD policy.
- 30% of the respondents were agreed that ineffective management issues results in the major cause of BYOD security in the firm.
- 26% of the respondents said that TYOD is the best mode of approaches in BYOD.
- 26% of the respondents using Mobile Information Management characteristics of security models for managing BYOD.
- 33% of the respondents were satisfied with BYOD policy.
- 29% of the respondents were using android under BYOD policy in the organization.
- 45% of the respondents said that proper infrastructure exists in place to support BYOD.
- 29% of the respondents said that sensitive data control method used in the firm for BYOD policy.
- 26% of the respondents were following audit devices BYOD policy.
- 27% of the respondents agreed that BYOD management & stipends cost more than just providing devices.
- 28% of the respondents agreed that the BYOD provides right balance between productivity and security.
- 26% of the employees said that URL filtering is used as the established security procedure to handle BYOD in the organization.
- 29% of the respondents neutrally said that the BYOD program is the right fit for the working organization.
- 25% of the respondents equally said that text messaging services and video calls were the work tasks they found useful to do on their own device in BYOD.

SUGGESTIONS AND RECOMMENDATIONS:

- To create a holistic and effective BYOD framework that ensures the security & privacy objectives of confidentiality, integrity, BYOD must elucidate the fundamental policies & standards of on-boarding and communication.
- Adopting and implementing an effective BYOD program is a responsibility that is not only restricted to IT network administrators but also it is a responsibility that should be undertaken by the firm and its employee in general.
- Intrinsically, an all-inclusive BYOD policy is required to ensure that the BYOD is not only efficacious but likewise secure. Here are some recommendations to aid organizations with their BYOD adoption.
- Policy considerations like Employee training on privacy awareness, Routine audit risk, Regular policy update encourages BYOD adoption in the firm.

- Corporate firms could also employ Virtual Private Network (VPN) to permit employees that remotely access IT infrastructure and to apply caution to avoid network attacks.

LIMITATIONS:

- The study is restricted to only 200 employees of Fabsys Technologies Private Limited.
- The information provided by the respondents could also be biased or inaccurate. No independent verification of the data was possible.
- Time is a major constraint.
- Information from more employees would have made this study more exhaustive but due to time limitations it is not possible.
- The respondents chosen were busy and have less time to answer the questionnaires.

CONCLUSION:

BYOD has become a good strategy that companies use due to their great benefits; companies like CISCO and others create technical solutions and implement policies to help mitigate the risks that comes with implementing this strategy. Bring Your Own Device policy security and privacy potential problems assessment is a significant move towards safeguarding the effective BYOD adoption, implementation, and management of confidential information in its framework. This work proffers unambiguous understanding of BYOD security risks and threats to adopters and users by identification and classification of possible list of threats/vulnerabilities of BYOD adoption that should be applied by firms and users to mitigate BYOD risks using a layered approach. According to the results of this study, notwithstanding that BYOD is an influential idea with the vast potential to strengthen productivity and effectiveness, organizations should adopt policies, procedures and standards that have the most fitting technical controls to avert organizational and employee's loss of confidential information. Technically, it is expected that the contribution of this research by implementation will be advantageous to employees and firms that use BYOD policies in the course of accomplishing its organizational goals. The use of BYOD is becoming widespread, and due to the security risks organizations should also have and enforce BYOD policies. One of the most important best practices is to balance the flexibility provided by BYOD with necessary security policies that do not negate the end user's abilities to perform their jobs.

REFERENCE:

- Ackerman, E. (2013). The bring-your-own-device dilemma: Employees and businesses seek to balance privacy and security. *IEEE Spectrum*, 50(8), 22–22. <http://dx.doi.org/10.1109/MSPEC.2013.6565553>
- Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, 42, 56–65. <http://dx.doi.org/10.1016/j.cose.2014.01.005>
- Armando, A., Costa, G., Verderame, L., & Merlo, A. (2014). Securing the “bring your own device” paradigm. *Computer*, 47(6), 48–56. <http://dx.doi.org/10.1109/MC.2014.164>
- Center for Public Issues Education. (2014.). Evaluating information sources. Retrieved from <http://ce.uoregon.edu/aim/Capstone1Perm/evaluateinfo.pdf>
- Chang, J. M., Ho, P.-C., & Chang, T.-C. (2014). Securing BYOD. *IT Professional*, 16(5), 9–11. <http://dx.doi.org/10.1109/MITP.2014.76>
- Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, 28(1), 209–226. <http://dx.doi.org/10.2308/isys-50704>
- Disterer, G., & Kleiner, C. (2013). BYOD Bring your own device. *Procedia Technology*, 9, 43–53. <http://dx.doi.org/10.1016/j.protcy.2013.12.005>
- Earley, S., Harmon, R., Lee, M. R., & Mithas, S. (2014). From BYOD to BYOA, Phishing, and Botnets. *IT Professional*, 16(5), 16–18. <http://dx.doi.org/10.1109/MITP.2014.69>
- Fiorenza, P. (2013). Mobile technology forces study of bring your own device. *Public Manager*, 42(1), 12–14.
- Ghosh, A., Gajar, P. K., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science*, 4(4), 62–70
- Johnson, K. & Filkins, B.L. (2012). SANS mobility/BYOD security survey. Retrieved from

- http://www.sans.org/reading_room/analysts_program/mobility-sec-survey.pdf
- Li, Q., & Clark, G. (2013). Mobile security: A look ahead. IEEE Security considerations. IT Professional, 14(5), 53–55. <http://dx.doi.org/10.1109/MITP.2012.93>
 - Mitrovic, Z., Veljkovic, I., Whyte, G., & Thompson, K. (2014). Introducing BYOD in an organisation: The risk and customer services viewpoints. Paper presented at The 1st Namibia Customer Service <http://ir.polytechnic.edu.na/handle/10628/522>.
 - Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD. Procedia Computer Science, 50, 511–516. <http://dx.doi.org/10.1016/j.procs.2015.04.023>
 - Webroot. (2014). Fixing the disconnect between employer and employee for BYOD (bring your own device). Retrieved from <http://www.webroot.com/shared/pdf/WebrootBYODSecurityReport2014.pdf>
 - Scardilli, B. (2014). BYOD or COPE: The best mobile strategy for the workplace. Information Today, 31(2). Retrieved from <https://www.questia.com/magazine/1G1-363515159/byod-or-cope-the-best-mobile-strategy-for-the-workplace>
 - Thomson, G. (2012). BYOD: Enabling the chaos. Network Security, 2012(2), 5–8.
 - Tokuyoshi, B. (2013). The security implications of BYOD. Network Security, 2013(4), 12–13.
 - Rivera, D., George, G., Peter, P., Muralidharan, S., & Khanum, S. (2013). Analysis of security controls for BYOD (bring your own device). The University of Melbourne, Australia. Retrieved from <http://hdl.handle.net/11343/33338>
 - Waterfill, M. R., & Dilworth, C. A. (2014). BYOD: Where the employee and the enterprise intersect. Employee Relations Law Journal, 40(2), 26–36
 - Marjanovic, Z. (2013). Effectiveness of security controls in BYOD environments. The University of Melbourne, Australia. Retrieved from <http://hdl.handle.net/11343/33346>
 - Jaramillo, D., Katz, N., Bodin, B., Tworek, W., Smart, R., & Cook, T. (2013). Cooperative solutions for bring your own device (BYOD). IBM Journal of Research and Development, 57(6): 5.
 - Hayes, B., & Kotwica, K. (2013). Bring your own device (BYOD) to work:
 - Marjanovic, Z. (2013). Effectiveness of security controls in BYOD environments. The University of Melbourne, Australia. Retrieved from <http://hdl.handle.net/11343/33346>
 - Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. Network Security, 2012(12), 5–8.

