An Empirical Investigation on Customer Adoption Intention of IoT (Internet of Things) in Commercial Banks of Lucknow

Abstract of Thesis

Submitted to

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY

(A Central University)

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
LUCKNOW
प्रज्ञा शील करूणा
ESTABLISHED 1996

for the Award of the Degree of

Doctor of Philosophy

in

Management

Submitted by

Neerja Rai

Enrollment No. 1699/19

Supervisor

Prof. Kushendra Mishra

DEPARTMENT OF RURAL MANAGEMENT
SCHOOL OF MANAGEMENT AND COMMERCE
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A CENTRAL UNIVERSITY) (NAAC A++ ACCREDITATION)
VIDYA VIHAR, RAEBARELI ROAD, LUCKNOW-226025
UTTAR PRADESH, INDIA

2023

Abstract

Introduction

During economic liberalisation and the introduction of new private-sector banks into the market, the banking sector has developed into one of the most competitive sectors in India. For the past few years, public sector banks have struggled to keep their operations running smoothly and meet client expectations. Everywhere you look, you can see how digitization and the IoT are developing and growing. Smart sensors and innovative digital services can be used in a variety of business sectors. The IoT and digital changes open up new possibilities for the world. IoT offers banks a range of benefits related to digital transformation, such as enhanced financial security, fraud detection, a 360-degree view of their customers, innovative insurance strategies, and more. The Internet of Things has enabled innovations that help banking and financial institutions deliver exceptional customer service and surpass client expectations.

Overview of Indian Banking

The banking system has been dominant in India since antiquity, and the Western commercial banking system was founded in the 18th century. In 1786, the General Bank of India was founded, becoming the country's first bank. Bank of Calcutta (1809), Bank of Bombay (1840), and Bank of Madras (1843) were all founded by the East India Company. The Hindustan Bank was created later in 1870. Presidency Banks were the names given to the three banks (Bank of Calcutta, Bank of Bombay, and Bank of Madras), which ultimately merged to establish the Imperial Bank of India in 1921. In 1935, the Reserve Bank of India was created after the Reserve Bank of India Act was

approved in 1934. To organise the operations and activities of commercial banks in India, the Banking Regulation Act was established in 1949. The regulatory legislation gave the Indian government jurisdiction over RBI. As a central banking organisation, the Reserve Bank of India has the jurisdiction to monitor and regulate the activities of Indian banks. No new bank or branch of an existing bank was permitted to open under the Banking Regulation Act without the RBI's permission. The Imperial Bank of India became a part of the RBI in 1955 and changed its name to the State Bank of India. In 1960, the State Bank of India's subsidiary of seven banks underwent nationalisation; in 1969, 14 significant commercial banks underwent the same process. In 1980, six further banks were nationalised, bringing the government's ownership of the banking industry to over 80%. The claimed purpose of nationalisation was to give the government more control over the provision of credit. With the second round of nationalisation, the government of India gained control of 91% of the banking industry, totalling 20 nationalised banks. The government's later 1993 merger of the New Bank of India and Punjab National Bank—the only such union of nationalised banks—led to the lowering of the total number of such institutions from 20 to 19. Early in the 1990s, the Narasimha Committee suggested financial reforms, and in 1993 it revised the Banking Regulation Act to allow foreign banks to operate in India. These financial institutions, which included ICICI Bank, HDFC, Axis Bank (formerly UTI Bank), and Oriental Bank of Commerce (previously Global Trust Bank), were referred to as new-generation technologically enabled banks. The banking sector was predicted to grow quickly as a result of the economic reforms and the loosening of restrictions on foreign direct investment (FDI), which altered the outlook of traditional banks. Four major periods can

be identified in India's banking revolution pre nationalization phase to the period of increased Liberalization. India's banking system is made up of cooperative and commercial banks. Private sector banks, foreign banks, and the nationalised State Bank of India and its affiliates make up the commercial banks. The public sector banks in India are made up of these banks and the local rural banks. As of 2015, 327 branches of 45 foreign banks were active in India, according to a study by the RBI. In India, 39 other banks have representative offices. Standard Chartered has the most locations among the international banks (101 locations), followed by HSBC (50 locations), City Bank (42 locations), and Royal Bank of Scotland (24 locations).

Technological Development in the Indian Banking Sector

The way that banks operate and how financial services are provided has changed as a result of technology. ICT (information and communication technology), wireless technology, and the widespread use of mobile and IoT devices have caused clients to visit bank branches less frequently and prefer to do banking activities at a time and location of their choosing. According to the Rangarajan committee report, the introduction of sophisticated ledger posting machines in the middle of the 1980s marked the beginning of the computerization process in India's banking industry. The Rangarajan committee, established in 1988, laid out a detailed plan in its second report for the computerization of banks and the expansion of automation into other domains including cash transfers and ATMs. With the introduction of ATMs, core banking solutions (CBS), branch automation, and the centralization of operations at the CBS in the late 1990s or early 2000s, the Indian banking industry began to see the advantages

of IT (Information Technology) projects. IDRBT (Institute for Development and Research in Banking Technology) was founded by RBI in 1996 with the goal of enhancing technology research and implementation in the banking and financial sector. Structured Financial Management System (SFMS), PKI-based electronic data transfer, NFS (National Financial Switch), SWIFT (Society for Worldwide Interbank Financial Telecommunication), and other technological infrastructures were developed to support secured payment practises in India (Rangarajan, 2011). The percentage of nationalised bank branches that were fully computerised at the end of March 2010 was 97.8%, compared to SBI's 100% computerization of all of its branches (RBI, 2010). With the development of ECS debit and credit transactions, internet banking in the early 2000s, RTGS in 2004, NEFT in 2005, and mobile banking in the late 2000s, the Indian banking industry transitioned from traditional cash payments to electronic payments in the late 1990s. According to research by the RBI, the number and value of transactions using cashless methods are increasing. Technological innovations are influencing consumer behavior, and banks must quickly adapt to these developments since it affects their ability to survive. The future of banking will be determined by three developments. Clients anticipate individualized banking services. There will be a significant increase in the amount of expectation for banks to provide personalized banking services. The function of artificial intelligence. Consider Chat GPT, which is revolutionizing the search industry by giving users what they want in a more organized way than conventional search engines like Google. Customers will also anticipate that banks will be aware of their responsibilities with governance, social, and environmental issues.

And banks who succeed in doing so will command a higher rate from clients (businesstoday, 2023) .

Introduction of the Internet of Things (IoT)

In the era of Industry 4.0, IoT and Smart Applications have become popular buzzwords. Internet and things together up the phrase "internet of things.". The Internet is a network of linked computer systems that communicate with one another using the Internet protocol (TCP/IP). It comprises a variety of networks connected by electrical, wireless, and optical technologies, including public, commercial, governmental, academic, and business networks. (Internet, 2015). Other than electrical equipment or gadgets, things are objects. Over the internet, electronic gadgets and equipment can communicate with one another. However, non-living things include things like clothing, food, furniture, tools, machinery, signs, plates, tubes, and household items like a refrigerator, TV, and microwave, while living things include people, animals, and plants. In supply chain management, Kevin Ashton first used the term "Internet of Things" in 1999 (businesstoday, 2023). In the last ten years, the definition has expanded to include a wider range of applications, including those in transportation, healthcare, agriculture, etc. In the IoT ecosystem, devices, sensors, and other things are linked together to relay data to a cloud computing platform. The cloud computing platform transforms the data into information, which is then transformed into knowledge, which is then transformed into wisdom for humanity. The global architecture of networked items or things that can be accessed anywhere at any time is known as the Internet of Things (Marek & Woźniczka, 2017).

Introduction of the Internet of Things (IoT)

In the era of Industry 4.0, IoT and Smart Applications have become popular buzzwords. Internet and things together up the phrase "internet of things.". The Internet is a network of linked computer systems that communicate with one another using the Internet protocol (TCP/IP). It comprises a variety of networks connected by electrical, wireless, and optical technologies, including public, commercial, governmental, academic, and business networks. (Internet, 2015). Other than electrical equipment or gadgets, things are objects. Over the internet, electronic gadgets and equipment can communicate with one another. However, non-living things include things like clothing, food, furniture, tools, machinery, signs, plates, tubes, and household items like a refrigerator, TV, and microwave, while living things include people, animals, and plants. In supply chain management, Kevin Ashton first used the term "Internet of Things" in 1999 (businesstoday, 2023). In the last ten years, the definition has expanded to include a wider range of applications, including those in transportation, healthcare, agriculture, etc. In the IoT ecosystem, devices, sensors, and other things are linked together to relay data to a cloud computing platform. The cloud computing platform transforms the data into information, which is then transformed into knowledge, which is then transformed into wisdom for humanity. The global architecture of networked items or things that can be accessed anywhere at any time is known as the Internet of Things (Marek & Woźniczka, 2017). Through a variety of services and applications, IoT offers significant benefits in daily activities. The following list of IoT's main benefits is provided:

- Improved Customer Commitment – Through a variety of consumer-supported services that track product quality as well as customer needs and satisfaction, IoT demonstrates improved customer engagement. It offers comprehensive, interactive, and user-friendly interfaces to identify product problems.

- Technology Optimization – Through the use of enabling technologies, IoT provides fast changes to the functionality of devices, software, and services. Based on device usage, demand, customer satisfaction, and current technologies, it enhances the products.

- Effective Resource Utilization – IoT-enabled efficient resource management. Once the resources and sensors are positioned over the application surface, any network topology and architecture may be accommodated.

- Enhanced Data Collection – Nowadays, the IoT platform offers a proactive method of gathering real-time data anywhere in the world. With the use of contemporary sensor technologies, the data can be gathered in a very brief amount of time. It can offer an analysis of the gathered data utilising algorithms with an artificial intelligence foundation.

Challenges and Constraints of the Internet of Things (IoT)

The IoT framework strongly supports Supply Chain Management (SCM) application (Fang et al., 2017). Previously, IoT was presented at the "World Summit on the Information Society (WSIS) Tunisia" in 2005. I0TGov encounters difficulties as a result of decreased effectiveness in safety, trust, hazards, and compliance, which exposes the

security. privacy of information and data, as well as the disclosure of confidential information. IoT operates in a diverse system since an IoT application integrates various technological tiers (Fishbein, 2015). The likelihood of security threats from potential hackers increases with the number of connected devices. The Internet of Things is more sophisticated than a flyover when you consider how involved it is. the gap between IoT management and governance in practical use. Customer safety and protection when utilising IoT solutions depend on quality assurance for IoT applications. It needs a high degree of performance testing and performance prediction due to the several billions of hardware and software components that are connected to the item. Despite many IoT benefits, there are certain obstacles and limitations facing contemporary IoT services. The following is a summary of some of the main obstacles and limitations facing IoT goods and services:

- Security – because the IoT puts a greater strain on the network and frequently faces security assaults due to the interconnectedness of billions of devices. The IoT architecture is expanding by many devices every second, making it challenging to monitor security.

- Privacy – The privacy of user information, data, and participation is occasionally breached by IoT.

- Complexity – The design, maintenance, and deployment of IoT systems are more difficult due to the deep structure of the IoT.

- Flexibility – Some IoT solutions are limited to a small number of devices and are unable to offer flexibility to numerous things. The ability to connect one Internet of Things technology with another is less flexible.

- Compliance – IoT compliance is difficult due to the lack of standard software compliance. With the use of various technologies, regulation, observation, and management become challenging.

Data Governance in Internet of Things (IoT)

The complexity of data collecting, storage, and processing rises due to the extensive usage of IoT in many applications, which also poses a number of data-related concerns requiring careful data governance. The relevance of data governance in IoT-enabled services is highlighted by Cha's study on the General Data Protection Regulation (GDPR), which focuses on data rights, confidentiality, and security in the IoT context. The difficulties of using data in an unethical way and reprogramming a device to perform tasks other than those intended are also emphasised. Data governance is crucial for the survival of an organisation since it grants corporate-wide decision rights and accountability for data quality control (Weber, 2010). Data governance encompasses information and data management, which develops a set of guidelines and rules to cover the entire life cycle of data, from collection through use and disposal. Data archival, replication, backup, safety governance council, data release, metadata management (MDM), data lineage, data traceability, business glossary mapping and master data, change management, and business are just a few of the procedures and standards that are defined by data governance to ensure effective and proactive handling and data

management regulation. IT governance and IoT data governance are two subcategories of data governance.

The supervision of IT assets like servers, networks, and applications through risk control and monitoring in alignment with societal policies and goals is what IT governance, which differs from data governance, is all about . Traditionally, governance was used to manage financial assets and services; but, in recent decades, it has only been applied to data and IT assets. There are several IT governance frameworks such as ISO 27001, “Information Technology Infrastructure Library (ITIL)”, and “Control Objectives for Information and Related Technology (COBIT)” (Gehrmann, 2012). IoT governance is an extension of IT governance that concentrates on IoT application lifecycles, IoT device data collection, and IoT device lifecycles in the governance landscape of any organisation. IoT governance is a sub-part of the existing IT governance landscape. It includes associations such as the Internet Engineering Task Force (IETF), Regional Internet Registry (RIRs), The Internet Corporation for Assigned Names and Numbers (ICANN), IEEE, Information Security Operations Centre (ISOC), Internet Governance Forum (IGF), or tailored IT governance frameworks offered to govern IoT (Almeida 2015). The distinction between data governance and governance of IT must be made apparent. Data governance has to do with data assets and the necessity to boost business results to meet stakeholder demands (Korhonen et al., 2016).

Internet of Things (IoT) And India

The industrial sector is evolving quickly according to SMACIT's strategy, which enables a digital revolution in every aspect of human life through linked and smart products,

powerful products, integrated business capabilities, and accessible technology. (Ross et al. 2016). IoT is a key component of SMACIT's strategy, and it is spreading quicker over the entire planet. The Auto-ID Centre at MIT originally demonstrated it in 1999 (Sharma & Sharma, 2019). When RFID-equipped devices are connected to the Internet and their data is shared to enable smart device management and identification, this is the application that the Internet of Things (IoT) starts to work.

By 2020, the Indian economy's IoT market is predicted to rise from its present $5.6 billion and 200 million connected units to $ 15 billion and 2.7 billion units. The Indian IoT market is anticipated to expand at a CAGR of over 28% between 2015 and 2020. The Indian government is taking the lead in formulating and drafting policies to realise the goal of creating a connected, secure, and smart system based on the requirements of our nation. Its main goal is to grow India's IoT market to $15 billion by 2022. By 2022, IoT revenue will mostly be driven by its industrial applications, particularly in logistics, automotive manufacturing, and transportation. Given that India hopes to gain 20% of the market in another five years, we can anticipate the global IoT industry to reach $300 billion by 2020. The IoT market in India now generates sales of $130 million per year. The Industrial IoT (IIoT), the expanding M2M communication market, the rising trend of wearable technology applications, and the growing acceptance of Cloud computing in IoT services are some of the key drivers influencing the IoT market in India. The largest IoT sector being served in India is the telecom industry. 36% or $47 million of the IoT industry's entire income in India comes from telecom. In terms of IoT revenues in India, the oil & and utilities industry comes in second with 29%, followed by

electronics with 29%. The three largest industries in terms of size are finance (banking), healthcare, and retail. These industries were slow to adopt the Internet of Things and generate revenue in the single-digit millions.

Internet of Things (IoT) and Bank

Technology has transformed the ways in which we communicate over the previous few decades. The way we engage with the environment around us has changed as a result of Wi-Fi and sensors. The new connectivity era is being ushered in by the Internet of Things. The idea of the Internet of Things is not new. Its exact origin is uncertain, however, it was probably coined to describe device connectivity and machine-to-machine communication in the late 1900s. Thanks to increased connectivity, we can now access the data collected, opening up a wide range of commercial possibilities as well as a number of personal benefits. Banks will play a key role in facilitating the majority of that potential. The way we interact with banks and the way they run their business will change. Branch locations won't be necessary because in-person services won't exist. Real-time bank transactions will be initiated by cars, homes, and offices. The bank's function as our money stewards will be expanded to include management services that aid their clients in financial planning, portfolio management, and even health. The bank can make better risk management decisions with more data gathered through IoT. Biometrics should aid in the verification process in all digital banking transactions with secure access, in addition to drawing on social media, spending, and other credit behaviour data. The only restriction on change is what we can imagine. Applications and services that will change the game are already being tested and used.

It's time for the "Internet of Things" to start offering financial services. One day, we might encounter the so-called Banking of Things (BoT). The banking sector has started looking for ways to use IoT's capabilities. According to a poll, 64.5% of worldwide banking executives keep track of their clients via mobile apps on smartphones, tablets, and other electronic devices. Additionally, 15.8% of banking organisations utilised IoT (Internet of Things) sensors in wearables to monitor client product consumption, 21.1% used digital sensors to collect product performance data, and 31.6% used the IoT (Internet of Things) to monitor retail locations (such as bank branches). While lenders are figuring out how to finance and manage the assets and their value collateral based on sensor data, banks have started utilising the IoT (Internet of Things) to monitor and gather data about their clients to know about financial transactions. In the near future, people are anticipated to begin making payments through linked gadgets. In the upcoming years, many financial executives predict that consumers will frequently conduct transactions utilising devices like smartphones or home appliances.

Public sector banks are crucial to the growth of the economy in our nation. Accepting deposits, the financial institution then uses those funds, either directly or indirectly through capital markets, to engage in lending activities. It links clients with capital shortages to clients with capital surpluses.

TECHNOLOGY ADOPTION THEORIES

An examination of its adoption is important given the development of technological breakthroughs. Technology adoption, according to research, is not solely influenced by technological factors; rather, it has evolved as a result of a much more complicated

process involving user attitude and personality dimensions (Venkatesh et al., 2003), social influence (Fishbein, 2015), trust (Gefen et al., 2003), and numerous enabling conditions (Thompson et al., 1991). Understanding the development of this area of Information Systems (IS) research and considering potential new areas for research are essential. One of the earliest areas of IS research is the model for technology adoption. In order to offer a thorough knowledge of their impacts on the adoption of technology, particularly in the banking industry, TAM models were the most well-known and widely recognised model (As-Sultan, S. Y., Al-Baltah, I. A., & Abdulrazzak, F. A. H. 2017). When Davis first introduced the TAM model in 1986, it was based on the Theory of Reasoned Action (Fishbein and Ajzen, 1980). Perceived usefulness (PU) and Perceived ease of use (PEOU), two key elements that influence an individual's acceptance and adoption of an information system, are explained by the TAM model. The IS model presented by DeLone and McLean (1992) with three key variable systems, quality, information/content quality, and service quality, was also utilised to determine the adoption of technology in addition to the technological acceptance model. While the organisational impacts evaluate effectiveness success, the system quality measures technical success, the information quality measures semantic success, user satisfaction, and individual impacts. The measurement of IS by Pitt, Watson, and Kavan (1995) includes service quality. As a result, the TAM model and the IS model were both employed to evaluate the technology adoption strategy.

➢ **Diffusion of Innovation Theory** (Rogers, 1983) In 1983, The diffusion of innovation theory, developed by Everett Rogers, was used to gauge how quickly

customers adopted new technologies. He divided the users into six groups based on four key factors: innovation, communication methods, time, and social system. These groups included innovators, early adopters, early majority, late majority, laggards, and leapfroggers. According to the hypothesis, a new approach or idea that is introduced at the beginning of the process is adopted at a lower phase, accelerating in the middle, and slowing down at the end. This is also known as the adoption epidemic model. Ajzen and Fishbein proposed the Theory of Reasoned Action (TRA) in 1975 as a result of this theory's failure to explain the behavioural motivation behind technology adoption.

➢ **Theory of Reasoned Action** (TRA) (Fishbein and Ajzen, 1975): Three variables were used in this 1975 hypothesis put forth by Fishbein and Ajzen: "Behavioural Intention (BI), Attitude (A), and Subjective Norm (SN)". The TRA theory emphasises how a person's attitude and subjective norms influence his or her behavioural intention. Mathematically, it is possible to say that attitude and subjective norms are added up to form behavioural intention. According to the hypothesis, if a person's BI towards adoption is strong, their intention will be translated into action.

➢ **Theory of Planned Behaviour** (Ajzen, 1985): The Theory of Reasoned Action (TRA), put forth by Fishbein and Ajzen in 1975, served as the foundation for the Theory of Planned Behaviour (TPB), which Icek Ajzen developed in 1985. The Perceived Behavioural Control (PBC), which refers to "people's perception of the ease or difficulty of performing the behaviour of interest," was the new variable added to the TRA theory. The prediction of behavioural outcomes by TPB overcame the flaw in TRA. The Self-

Efficacy Theory (SET), first suggested by Bandura in 1977 and derived from Social Cognitive Theory, is the foundation of the PBC concept.

➢ **Technology Adoption Model**: The Theory of Reasoned Action (TRA) developed by Ajzen and Fishbein is expanded upon in TAM. The most extensively used model of users' adoption and use of technology is Davis's technology acceptance model (Davis et al., 1989) (Venkatesh, 2000). The two technology acceptance metrics—perceived usability and ease of use—TAM replace TRA's attitude measurements. The TAM model, which uses actual technology use as its goal, explains how a user adapts to a new technology. The original Davis (1989) study was duplicated by other researchers to show the connections between the usefulness, usability, and practical use of technology (Adams et al., 1992); (Hendrickson et al., 1993); (Segars & Grover, 1999);(Adams et al., 1992); (Szajna, 1994). Many academics tested the technology acceptance model variable. (Byun et al., 2018); (Gao & Bai, 2014); (Legris et al., 2003); (Wu & Wang, 2005). And identified that TAM aids in comprehending and forecasting the user's adoption of information systems. (Legris et al., 2003). TAM was thus used in a variety of fields, including internet services. (Liao et al., 1999), M-commerce (Ervasti & Helaakoski, 2010);(Mallat et al., 2009) , social networking (Rauniar et al., 2014), e-health care services (Holden and Karsh 2010), and mobile payments (Liébana-Cabanillas et al. 2014; Ramos-de-Luna et al. 2016). Numerous studies have demonstrated that Davis' (1989) construct has good validity and reliability and that the variable accurately predicts attitudes towards system utilisation. (Adams, 1992;

Hendrickson et al., 1993; Szajna 1994) Two crucial factors that characterise how technology is really used are suggested by the TAM model.

• **Perceived Usefulness** (PU) – As defined by Fred Davis, "the degree to which a person believes that using a particular system would enhance his or her job performance". It refers to whether the technology will help them do their task.

• **Perceived Ease-Of-Use** (PEOU) – In Fred Davis's words, "the degree to which a person believes that using a particular system would be free from effort" refers to whether or not consumers find the technology simple to use and have a favourable opinion of its actual application. The TAM model has continuously expanded throughout the years. TAM 2 (Venkatesh & Davis 2000) and UTAUT (Unified Theory of Acceptance and Use of Technology) (Venkatesh et al. 2003) were the two primary improvements. From the standpoint of e-commerce, TAM 3 was presented with the trust and perceived risk variable on actual use. (Venkatesh & Bala, 2008). Considered key influences on actual technology use were social influence, the utilitarian hedonic component, and perceived value. (Holbrook, 1999).

➢ **Extended TAM2 model** (Venkatesh et al., 2000): Venkatesh et al. revised TAM by including additional determinants of Cognitive instrumental processes (work relevance, output quality, outcome demonstrability, and perceived ease of use) and social influence processes (subjective norm, voluntariness, and image). The social influence determines the influence of peer on individuals' acceptance and rejection of a system. Venkatesh and Davis included the cognitive determinants in TAM2 along with social influence.

The extended TAM suggests that the subjective norm influences the image as the theory states that using a system will elevate the individual's image. Additionally, TAM 2 theorizes that prior to implementation and during early usage, there will be a large direct effect of subjective norms on intentions to use in required usage scenarios. The TAM2 model includes a number of factors that influence perceived usefulness, including job relevance, output quality, outcome demonstrability, and perceived simplicity of use. The ability of the system to support a person's job function determines the relevance of a job. Venkatesh and Davis described "output quality as an individual's perception of how well the system performs a specific task". Result demonstrability implies that individuals will have a more positive attitude about the system's usefulness if the differences between usage and positive results can be easily observed. Moreover, perceived ease of use examines how easy or effortless a system is to use. Venkatesh and Davis asserted that TAM2, which proposes that all cognitive instrumental processes positively influence perceived usefulness, ultimately influence an individual's intention to use an information system. Overall, once the adoption of a system moves beyond an individual decision to a team decision, social influence processes must expand beyond TAM2. Perceived innovativeness Perceived innovativeness is a domain-specific individual trait that reflects a person's willingness to try out new information technology. Based on the Rogers theory of diffusion of innovation, Agarwal and Prasad (1997) argued that individuals develop faith in new technology by synthesizing the information. Personal 13 innovativeness symbolizes the risk-taking propensity of individuals in adopting innovative technology. This trial was also named as personal innovativeness in information technology PIIT and also included as a new construct in

Davis's original TAM model. They have also highlighted that individual with higher level of PIIT are expected to develop more positive intentions towards the adoption of IT/IS. In the year 2000 Agarwal and Karahanna developed a multidimensional construct labelled cognitive absorption and emphasized that this innovativeness could be an antecedent of the two commonly recognized behavioural attributes: perceived usefulness and perceived ease of use. Thus, for the adoption of IS, innovation such as wireless mobile technology innovativeness plays an important role. Unified Theory of Acceptance and Use of Technology (Venkatesh et al., 2003): Venkatesh et al. proposed this theory, also known as UTAUT, in 2003 after conducting a thorough analysis and combining the concepts from the previous eight theories. (TRA, TAM, MM, TPB, TAM2, DOI, SCT and model of personal computer use). It is intended to function as a thorough model that is adaptable to many application scenarios. There are four main components to it namely "performance expectancy, effort expectancy, social influence and facilitating conditions" which are accommodated in developing the unified model. After compiling and evaluating every construct from earlier models, the authors hypothesised that the four characteristics listed above, out of the seven previously utilized, are the most important predictors of intention to use information technology. The remaining three constructs—technological attitude, self-efficacy, and anxiety—are thought to be fully mediated by ease of use, which is taken into account in the unified model as performance expectancy, and therefore not direct determinants of intention. This means that the UTAUT model no longer includes these three constructs. The unified theory's constructs are better since they account for 70% of the variance in adoption behavior, compared to the preceding theories' 30–40% explanation.

(Venkatesh et al., 2003). It is criticized, meanwhile, for being unduly complex, not taking a frugal approach, and not being able to explain individual behavior. (Casey & Wilson-Evered, 2012); (Liao et al., 1999). (Rosenbaum et al., 2011) conducted a thorough review of 450 publications that cited UTAUT and discovered that only few of them actually employed the constructs of UTAUT in their research. Researcher has reviewed approximately 100 research papers from the year starting 1999 to 2021. Through literature, researcher has understood the concept well and also assessed the past work done by various authors on the same. This review has helped the researcher in determining theoretical base and nature of the study. These studies helped the researcher in finding path of her research based on previous work.

Research Gap

While there is a growing literature which defines the IoT's recent development with its social, economic and behavioral aspect for the society, there are only limited papers describing IoT (Internet of Thing), as a next phase of digital revolution which will replace traditional banks. Very few papers study the awareness, adoption and impact of IoT on banking sector, their customers and the economy. Relative to the existing literature, therefore, this study focuses on adoption intention of customer towards IoT (Internet of Thing) in commercial banks.

Research Methodology

The research methodology has been decided after reviewing literature available on influencing factors of adoption intention of customer towards IoT (Internet of Thing)

Banking. Literature has helped the researcher in determining theoretical base and nature of the study. Research is a mixture of qualitative and quantitative research techniques. Research design of the study is exploratory in nature. The sample size is about 504 respondents. Data is collected after conducting pilot study on 50 respondents of Uttar Pradesh. Sampling technique is based on Stratified sampling method. Data has been collected through survey method. Online questionnaire is prepared to collect the data from various respondents of Lucknow (Uttar Pradesh). Analysis of the data has been done on SPSS 23.0 version and on AMOS 23. Suitable statistical methods have been applied for the analysis of the data. Research methodology of the topic is divided into following sections: Research questions, Objectives of the study, Hypothesis formulation, Research Design and type of research, Research Approach, Data Collection and questionnaire designing, sampling design with sampling plan, Population of the study, sampling frame, sampling unit, sample size, sampling technique, Data analysis tools.

Research Objective

1. To identify the various factors influencing the awareness and adoption intention of the Internet of Things (IoT) in Commercial Banks of Lucknow.
2. To investigate the issues and benefits related to the banking services employing IoT (Internet of Things).

Formulation of Hypothesis

$H0_1$: There is no significant effect of Social Influence on customer adoption of IoT Banking.

$H1_1$: There is a significant effect of Social influence on customer adoption of IoT Banking.

$H0_2$: There is no significant effect of Perceived Usefulness on customer adoption of IoT Banking.

$H1_2$: There is a significant effect of Perceived Usefulness on customer adoption of IoT Banking.

$H0_3$: There is no significant effect of Perceived Ease of Use on customer adoption of IoT Banking.

$H1_3$: There is a significant effect of Perceived Ease of Use on customer adoption of IoT Banking.

$H0_4$: There is no significant effect of Financial Literacy on customer adoption of IoT Banking.

$H1_4$: There is a significant effect of Financial Literacy on customer adoption of IoT Banking.

$H0_5$: There is no significant effect of Trust on customer adoption of IoT Banking.

$H1_5$: There is a significant effect of Trust on customer adoption of IoT Banking.

$H0_6$: There is no significant effect of Privacy and Security on customer adoption of IoT Banking.

$H1_6$: There is a significant effect of Privacy and Security on customer adoption of IoT Banking.

Proposed Research Model

Drawing on the existing body of literature, it identifies six constructs, which posit to have an influence on the intention to use mobile banking (Figure 3.1). the independent variables/factors which are used in this study include perceived ease of use, perceived usefulness, social influence, trust, privacy and security and financial literacy.

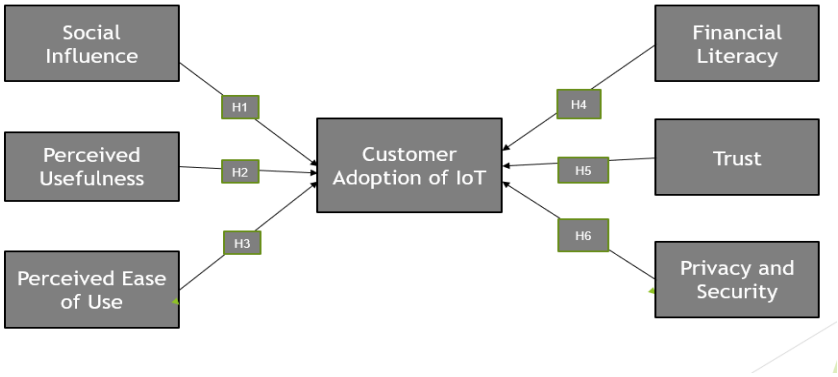

Fig 3.1: Proposed Research Model

The research model developed for the present study derived the constructs from the existing technology adoption models such as the Technology Acceptance Model (TAM) (Davis, 1989), the Decomposed Theory of Planned Behavior (DTPB) (Taylor & Todd, 1995), and Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al, 2003). The study added constructs such as trust and security which are relevant to understand IoT banking acceptance.

A measurement model based on the idea of planned behavior combines all of the latent dimensions with their maintained indicators. The measuring model is shown in Figure 4.14. Since all of the values in the measurement model are larger than.5, they are all

considered significant and after doing CFA, SEM has been applied on the data. As shown by figure 4.15.

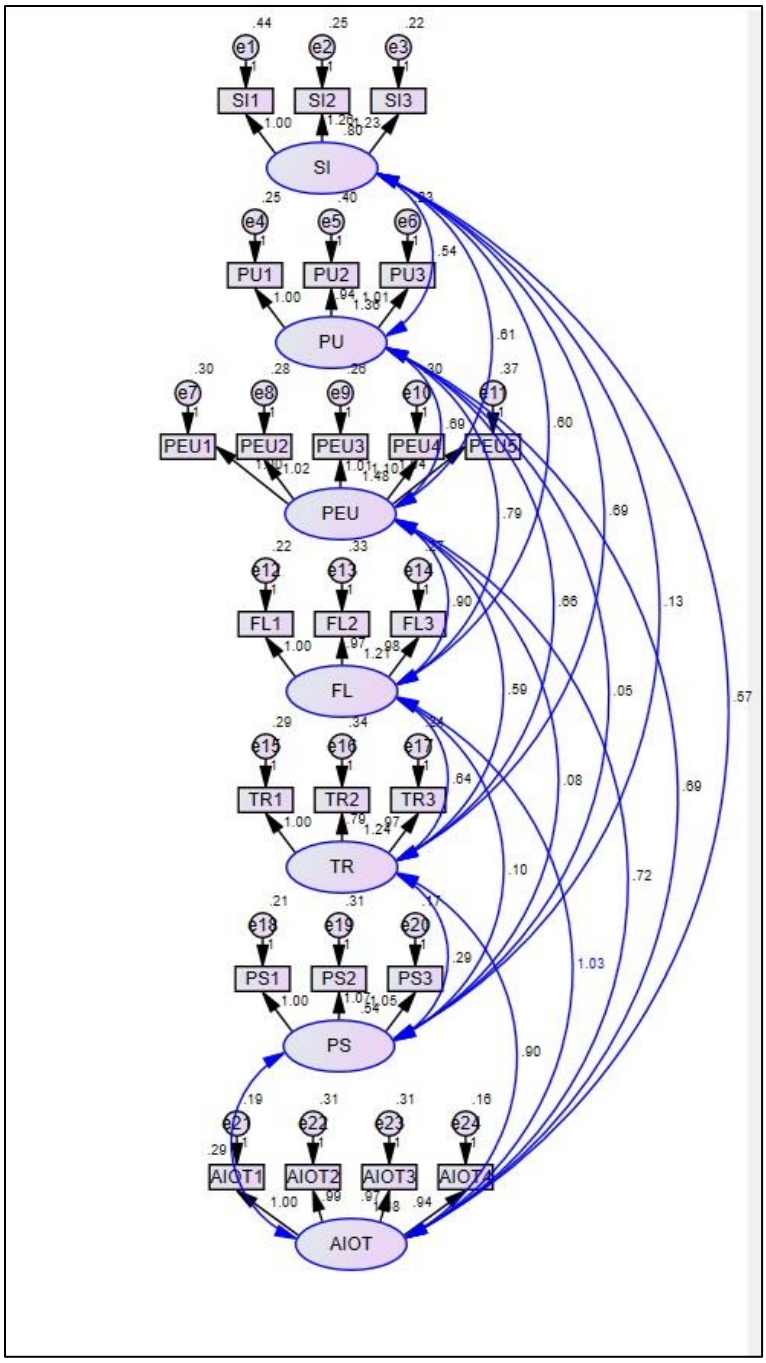

Fig 4.14: Measurement model of the data

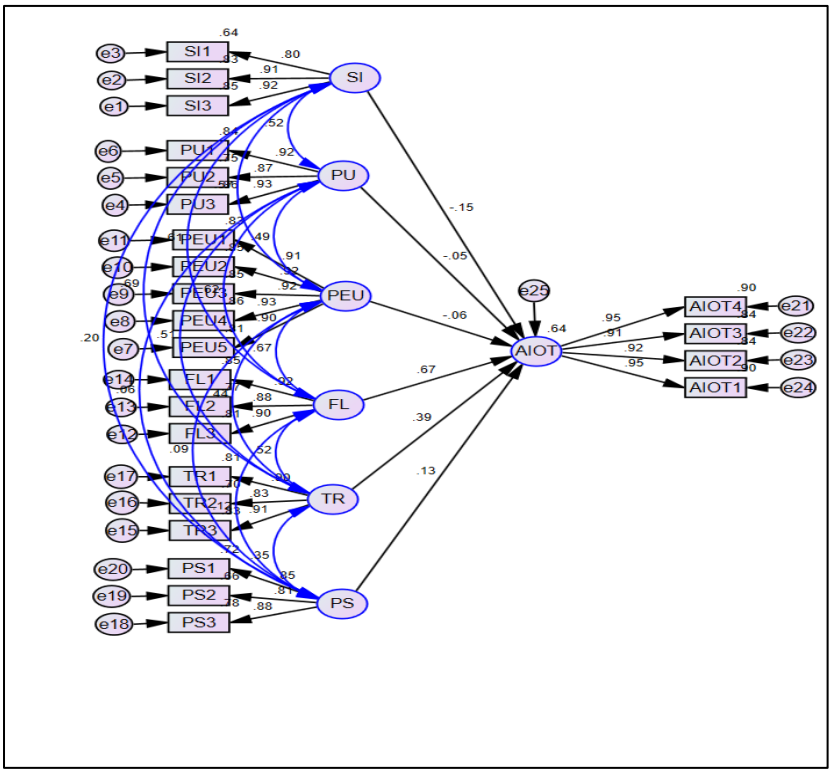

Fig 4.15 Structural Model of the Data

Result of the Analysis

Null Hypothesis	Result	Alternate Hypothesis	Result
$H0_1$	accepted	**$H1_1$**	rejected
$H0_2$	accepted	**$H1_2$**	rejected
$H0_3$	accepted	**$H1_3$**	rejected
$H0_4$	rejected	**$H1_4$**	accepted
$H0_5$	rejected	**$H1_5$**	accepted

$H0_6$	rejected	**$H1_6$**	accepted

Findings

The first objective of the study was to identify the variables that affect Indian bank customers' adoption of IoT banking. The current study's empirical findings highlighted six variables that affect customers' intentions to utilize IoT banking, including perceived ease of use, perceived usefulness, social influence, financial literacy, trust, privacy and security. The hypotheses H3, H4, H5 and H6 outlined the relationship between these variables and the uptake of IoT banking. All of these hypotheses were proven correct, which shows that Indian banking clients saw these characteristics as being of the utmost importance when considering the use of IoT banking. Consumers place great value on an intuitive, user-friendly experience while doing banking transactions online. Since IoT banking is a novel technology-enabled service to Indian banking customers.

The second objective of the study was to explain the benefits and issues of employing IoT banking services. The results showed no substantial difference in the intentions of males (50.2%) and females (49.8%) to utilize IoT banking services and also found that there was a significant variation in different age groups for adopting IoT banking as the majority of respondents (90.1%) between 20-40 age group then to another age group (7.3%). Because financial sectors handle money and private information, the banking industry is highly sensitive. The study also reveals that different constructs as Trust,

privacy and safety in their order of influencing power, where the factors influenced the customer's intention to adopt IoT banking. Businesses using the Internet of Things in the banking sector run serious dangers to their privacy and security. Because the Internet of Things is portrayed as a huge network of hardware and software, hacking risks are increasing. Another way to think of the Internet of Things is like a chain, where links are essential to keeping connectivity strong. The chain breaks as a whole if one link is broken. It has an impact on both the software and the hardware. Customers want banks to have stronger security measures, as evidenced by this, particularly when using a wireless network where they anticipate privacy and transaction security.

Conclusion and Suggestions

The study's goal was to identify the variables that have an impact on banks' adoption of the Internet of Things (IoT). To accomplish the aforementioned research objectives, a sequential mixed approach was employed. The hypothesis was developed and a research model was suggested using the first exploratory qualitative study approach. The second descriptive study approach was used to test the hypothesis and use a quantitative approach to validate the suggested model. To ensure that the findings could be applied to the entire population, a sizable sample size of 504 participants was used in the study. The fact that these mixed-method studies combine the results from both the qualitative and quantitative phases of the research lends evidence to their developmental nature (Venkatesh et al., 2013). According to the results, the adoption of IoT is greatly impacted by privacy and safety; as there is no danger involved in using this technology, privacy and safety are regarded as important factors. The information that Indian banks are

sharing over the Internet of Things has an impact on them. This indicates that since financial information is very private, there are extensive safety considerations for bank clients. Moreover, the findings suggest that trust plays a role in the Internet of Things' uptake in Indian banks. It is intended for people to use IoT banking services if they receive regular information, are given access to real-time data, and are offered value-added services that meet their needs.