IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 6, June 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106032 |

Analysis of Consumer Behavior Using Internet of Things

Mr Abdul Razzak Khan Qureshi[1], Dr. Jitendra Sheetlani[2]

Research Scholar, SSSUTMS, Sehore (M.P.), India[1]

Associate Professor, SSSUTMS, Sehore (M.P.), India[2]

ABSTRACT: The Internet of Things (IoT) connects everyday electronic gadgets (such as security cameras and smart TVs) to the internet in order to increase their usefulness and efficiency. However, substantial security and privacy issues concerning the IoT have been highlighted, affecting customer trust and purchase decisions. Furthermore, gadgets range significantly in terms of security, making it difficult for users to distinguish between better and less secure devices. We describe a research of customer behaviour and purchase behaviour when using internet of things (IoT) devices in this paper. In addition, the characteristics, benefits, drawbacks, and goals of the Internet of Things are discussed.

KEYWORDS: Internet of Things, Security and Privacy, Threats, Consumer behavior, purchasing.

I. INTRODUCTION

Understanding customer behaviour has always been critical for gaining market share and cultivating loyalty. However, as items grow more commoditized and diverse businesses become increasingly competitive, knowing customer behaviour has become critical to surviving in a crowded industry. From customer relationship management systems to marketing automation software to customer personalization tools and more, there is no shortage of tools and systems geared to understand your customers' behaviour. Understanding client behaviour, on the other hand, necessitates data and computational power [1]. The cloud computing architecture isn't well suited to real-time data analysis and heavy processing. Alternative approaches to cloud computing are required for data- and compute-intensive enterprise tasks.

Organizations have taken their quest to the streets, or, to be more precise, to the enterprise edge. Devices, programmes, and data may be accessible at the edge without having to travel to the cloud. This allows for faster data processing and, potentially, more secure data access. As a result, smart linked devices including Internet of Things (IoT)-enabled sensors and mobile devices, as well as AI-driven applications, can be better utilised. As they make crucial business decisions, businesses can obtain faster access to data and analyse that data.

The edge was born out of necessity, and its evolution was a natural result of its logistical implications. Hundreds of thousands of cloud-based applications have emerged, and billions of IoT devices have entered the world as the cloud has become the platform of choice. This massive disparity in growth rates has resulted in two major IoT deficiencies: a lack of processing capacity where things are actually happening, and a lack of time to wait for centralised computing infrastructure to handle the outcomes of these data-intensive activities [2].

The function of mobile computing has been substantially extended thanks to IoT devices. They've come to define it, to the point where many, if not most, people prefer to use apps while standing rather than sitting. Because of the increasing mobility and the requirement for speed, processing resources have been shifted from the cloud to the edge, where they are desperately needed

It's difficult to exaggerate the significance of this enhanced computing capacity; it enables organisational decision-making to be flexible and responsive not only at headquarters, but also on the go. Sensors, smart cameras, and other various endpoints (together with the devices users carry) are fundamentally changing IT in retail, warehouses, factories, and even private residences. Our understanding of IT systems and the applications that they generate is changing all the time. To some extent, this evolution has been self-determining; however, as new infrastructure is introduced into old systems – that is, as they are extended to the edge – the ability to guide that evolution is rapidly rising.Warehouses and factories have become self-monitoring, regulating their own energy usage, and doing self-maintenance, and are now working toward self-optimization. Inventories, which are currently digitally tracked, will eventually be completely self-managed [3]. The customer experience at the point-of-sale is becoming increasingly automated; it is intended to be self-scaling and, where appropriate, customer-individuated, with amenities personalised to the buyer. The Internet of Things (IoT) has now bridged the gap between the physical world and the digital universe that accommodates it. The traffic on that bridge is directed by AI. We can anticipate a rapid increase in the sophistication of these relationships. Smart cameras and beacon technologies in a store can optimise these settings based on motion detection; they will soon study body language and facial emotions and adopt benign contrivances to change a negative consumer experience into a

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106032 |

positive one. A completely new demography is forming, one that will optimise and tailor the customer's experience far beyond what browser/click tracking or social media monitoring could ever do. Understanding customer behaviour arises at the edge, and leveraging this knowledge will result in more successful marketing, customer service, communication, apps, and corporate processes.

II. REVIEW OF LITERATURE

2.1 IoT security and the consumer: the challenges and education

When the Internet first became popular, the Belgian government commissioned us to create a website to educate consumers and businesses about security dangers and precautions to take when using the Internet. It was part of a large-scale public awareness effort. It's as though we've returned to that stage with the Internet of Things, albeit in a consumer electronics and consumer IoT setting. The stakes, on the other hand, are substantially larger. Even today, a significant number of people use the Internet without the necessary security protections. Sure, they have some software, but it's not much, and it's rarely updated. Even yet, you can't compare today's situation to those of the past. Consumers are generally more aware of the dangers of the Internet, social media, and other online platforms. The same can be said for enterprises, where we are finally seeing holistic security measures (by definition, the only feasible approaches) get more and more attention. However, as you will see and read, there is still much work to be done. Furthermore, with the holiday season rapidly approaching and recent IoT vulnerabilities and DDoS attacks in mind, now is the time to pay attention, especially in the context of connected devices and the Internet of Things in a consumer context. [4].

2.2 Security and data privacy challenges are more critical than ever in human history

Cybersecurity – as well as data privacy – are serious issues. They've never been. They are, nonetheless, crucial in a data-driven digital transformation economy for the ways we work, consume, conduct business, and live. You've probably heard the adage that data is the new oil. "Data is the new oil, and data breaches are the new oil spills," said Deloitte's Dana Spataru during the IoT Solutions World Congress in Barcelona in late October 2016. I'd add that not everyone agrees on who owns the oil and who is responsible for it. At the same time, hackers and attackers are increasingly working in organised cybercrime groups, and attacks are becoming more complex, with over 60% of advanced threats arriving via encrypted traffic, necessitating a newcybersecurity approach.Furthermore, governments and supranational institutions are progressively regulating data privacy and personal data processing, as is the case with the EU's upcoming General Data Protection Regulation (GDPR) and its hefty fines and penalties, as well as the Privacy Regulation [3].

While attitudes toward data privacy and ethics vary by location and individual, expect more initiatives in an age where data – and the value we derive from it – is at the heart of the Internet of Things and data is a vital economic asset in a DX economy. In the end, a government's job is to safeguard its population, which includes data in the digital era. It's no surprise that de facto regulation is a thingis a key driver of the security market.

2.3 Time to get real about consumer IoT security: rotten apples and the human factor

Of course, business groups, local government awareness programmes, and a variety of other organisations are all working to improve security, as I noted before. This is certainly true in the IoT market, where security measures appear more frequently than before. In the consumer arena, one example is the Z-Wave Alliance's development of a new S2 framework (Z-Wave is a smart home standard) that is essential for any suppliers who seek Z-Wave certification after April 2, 2017. However, let's face it: not every vendor is as concerned about security as they are about profit, especially if they are not employing standards where security is a requirement for certification. This is a problem for the industry. You've heard the story about the barrel of apples with a few bad apples in it. Regulators eventually come in, as we've seen so many times in many domains. Whatever your feelings about legislation and industry initiatives, it's a well-known fact that some of those (typically less expensive) gadgets are manufactured by companies that fail to consider the most basic aspects of security. However, there is no way for the common consumer to know, and there is no means to return these items to their original countries. Over half of IoT device manufacturers will be unable to address vulnerabilities posed by inadequate authentication procedures by the end of 2018. (Gartner).But, again, with the Internet of Things the stakes are higher, much higher [4].

2.4 The IoT device and IoT security budget challenges at hand

If we want to actualize all of this, we'll have to wait a long time, if we ever get there at all. Because, according to Gartner, IoT will account for barely 10% of security budgets by 2020, despite the fact that it is expected to account for over 25% of recognised enterprise assaults by 2020. Why should it be deemed significant in general if it isn't in

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106032 |

organisations? The industry can help, but it can't solve all of the problems. The situation is made worse by the fact that, according to Gartner, until 2018, over half of IoT device manufacturers will be unable to address dangers posed by inadequate authentication procedures [3].

It's certainly no accident that, with the 2016 holiday season in mind, associations and vendors are ramping up their marketing and communication efforts to remind us, as consumers, reporters, and analysts, that customers aren't well-versed in IoT security or security in general. Only 42% of consumers take proper security steps to protect their new gadgets, according to a press release and new infographic (see below) produced by McAfee (Intel Security) during the 2016 holiday season. In addition, there are visibly connected devices among these equipment.Drones, smart home gadgets, and other Consumer IoT devices all pose a threat, and not simply to the misinformed or untrustworthy consumer. By 2018, 16 percent of the population will be Millennials, and their reality of a connected world will accelerate IoT adoption (IDC). After all, the Internet of Things era is one of hyper-connectivity. What is certain is that the consumer is impatient, with McAfee finding that 79 percent of consumers use connected gadgets on the first day they receive them. Based on the press release, the graph below depicts the disparities in consumer awareness of vulnerabilities between some "older categories" and "newer" connected products.

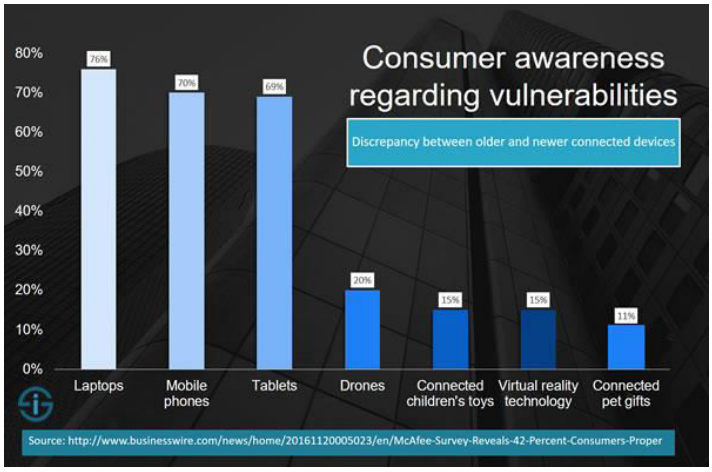

Fig. 1Consumer awareness regarding vulnerabilities

Moreover, only 42 percent of consumer claim they take the proper security measures and while most consumers realize it is important to secure their devices, 47 percent are certain if they are taking the proper measures to do so.

Fig.2 : Hackable 2016 holiday gifts

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106032 |

According to IDC, by 2018, 16 percent of the population will consist of the demographic cohort we called 'Millennials' and that should accelerate IoT adoption [4].

III. CONSUMER ATTITUDES TO IOT DEVICES

As this analysis on IoT security and privacy demonstrates, consumers' mostly negative perceptions of the IoT have significant repercussions. For starters, manufacturers and retailers must do a better job of assuring that Internet of Things devices provided to consumers are thoroughly tested for data collection and transmission. For example, in the United Kingdom, there is rising support for a mandatory labelling plan that would compel all IoT devices to include a warning label that explains how and why data is gathered. If merchants and manufacturers are unable to tackle all of the IoT security and privacy concerns, the industry's momentum may be stifled. For example, the survey found that 28% of people who do not already own a connected device are hesitant to get one in the future due to concerns about IoT security and privacy. It's worth recalling the early days of Internet e-commerce here. Concerns that hackers would gain access to credit card and payment information plagued the early e-commerce sites. As a result, security certificates and other "evidence" that a website was safe to use were developed. The same type of "evidence" may be required for linked devices in the future. Otherwise, consumers will continue to be concerned about all the negative consequences of using these products [5].

Trust in the IoT

So, who should be in charge of resolving all of these IoT security and privacy concerns? When The Internet Society addressed this question, 88 percent of respondents replied regulators, followed by manufacturers (81%), and retailers (81%). (80 percent). As a result, while the government may be able to intervene and regulate changes, it will also take the active participation of manufacturers and retailers to advance IoT security and privacy initiatives.

The report's one silver lining is what the authors refer to as "the trust opportunity." Manufacturers have the chance to exploit IoT security and privacy to gain a competitive advantage in the marketplace. In other words, if businesses can demonstrate that they are building IoT security and privacy into their devices from the start, consumers will regard them as more trustworthy and be more willing to buy their products. [6].

Going forward, there appears to be a clear link between consumer knowledge of IoT security and privacy risks and the level of market regulation. As a result, it is almost certain that more IoT-related regulation will be implemented in the near future.

There are four main components used in IoT:

- Low-power embedded systems
  Less battery consumption, high performances are the inverse factors play a significant role during the design of electronic systems.
- Cloud computing
  Data collected through IoT devices is massive and this data has to be stored on a reliable storage server. This is where cloud computing comes into play. The data is processed and learned, giving more room for us to discover where things like electrical faults/errors are within the system.
- Availability of big data
  We know that IoT relies heavily on sensors, especially real-time. As these electronic devices spread throughout every field, their usage is going to trigger a massive flux of big data.
- Networking connection
  In order to communicate, internet connectivity is a must where each physical object is represented by an IP address. However, there are only a limited number of addresses available according to the IP naming. Due to the growing number of devices, this naming system will not be feasible anymore. Therefore, researchers are looking for another alternative naming system to represent each physical object.

Characteristic of IoT

- Massively scalable and efficient
- IP-based addressing will no longer be suitable in the upcoming future.
- An abundance of physical objects is present that does not use IP, so IoT is made possible.
- Devices typically consume less power. When not in use, they should be automatically programmed to sleep.
- A device that is connected to another device right now may not be connected in another instant of time.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106032 |

- Intermittent connectivity – IoT devices aren't always connected. In order to save bandwidth and battery consumption, devices will be powered off periodically when not in use. Otherwise, connections might turn unreliable and thus prove to be inefficient.

1.2 Advantages of IoT

Internet of things poses various advantages in different area of sectors like:

- Communication
- Automation
- Remote Control
- Better Decision
- Money control
- Time Saving
- Continuous Monitoring
- Efficient handling

Disadvantages of IoT

- Lagging of standard compatibility
- More opportunities for failure
- Loss of privacy or security
- More dependent on technology

The internet of things is more vulnerable to various types of security threats due to their ad hoc nature so it becomes the challenging task for us and to mitigate or combat various techniques has been developed.

IV. SECURITYGOALS OF INTERNET OF THINGS

Traditional security goals, known as the CIA-triad, are grouped into three primary groupings in the literature: I confidentiality, (ii) integrity, and (iii) availability. Confidentiality: It assures that only authorised objects or people have access to sensitive information. With the emergence of the Internet of Things, it is critical to ensure the security of IoT gadgets, as they may handle sensitive data such as credit cards and medical records. For example, the authors in [8] show how permitted access to medical objects might expose personal information or lead to life-threatening situations. Integrity is also necessary in the IoT environment for offering dependable solutions in which only valid commands and data are received. Compromise of integrity might have negative repercussions. For example, the authors in [9] disclose successful assaults on an Insulin Pump that can divulge patients' personal information. IoT availability [10] is critical for ensuring that IoT services are available and unaffected. Despite the CIA-popularity, triad's the authors of [11] demonstrate its inadequacy in dealing with unexpected dangers that emerge in a collaborative context. To address this problem, they developed the information, assurance, and security (IAS) octave, also known as the IAS-octave, by reviewing a large amount of security-related information in the literature. Table 1 highlights the security goals suggested by the IAS-octave, along with their definitions.

Table 1. Security goals of IoT [12]

Security Requirements	Definition
Confidentiality	The process in which only authorized objects or users can get access to the data
Integrity	The process in which data completeness, and accuracy is preserved
Non-repudiation	The process in which an IoT system can validate the incident or non-incident of an event
Availability	An ability of an IoT system to make sure its services are accessible, when demanded by authorized objects or users
Privacy	The process in which an IoT system follows privacy rules or policies and

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106032 |

	allowing users to control their sensitive data
Audibility	Ensuring the ability of an IoT system to perform firm monitoring on its actions
Accountability	The process in which an IoT system holds users taking charge of their actions
Trustworthiness	Ensuring the ability of an IoT system to prove identity and confirm trust in third party

4Consumer Purchase Behaviour

The set of decisions people make and the activities they perform when buying and using a product is referred to as purchase behaviour [1]. Need recognition, information search, pre-purchase alternatives evaluation, purchase, consumption, post-consumption evaluation, and divestment are the seven stages of purchasing [2]. Pre-purchase behaviour entails determining what to buy and when to acquire a product [3], but post-purchase behaviour is comparing a product's expectation to its observed reality and managing concerns and unhappiness [4]. Consumer decision in the pre-purchase evaluation stage is influenced by a number of factors, according to researchers. Price, brand, features, aesthetics, and usability, for example, all impact mobile phone purchasing [5, 6, 7]. Consumers' buying intentions are mostly influenced by the perceived quality of a product [13]. Consumer purchase behaviours have been proven to be influenced by digital and social media [14]. Furthermore, reviews and word of mouth have been found as crucial variables [15, 16]. We observed the impact of several of the above mentioned aspects on people's IoT device purchasing decisions in our interview study. People are concerned about the protection of their personal data when making online transactions, according to studies [17]. Consumers are more inclined to purchase from privacy-protective websites, even if they are more expensive, according to Tsai et al. [18], when accessible privacy information is made available in search results. Kelly et al.found that adding concise privacy information to a mobileapp store can impact users**' app-selection decisions [19]**.

Labels

Labels have long been used to provide information to customers before they make a purchase. In the United States, for example, consumers can evaluate the nutritional content of food products using nutrition information labels, or compare the energy efficiency of light bulbs using Lighting Facts labels. Furthermore, academics have created privacy labels for websites, which have been proven to be preferred by users over typical privacy policies [20]. Many consumers are concerned about the privacy and security of their IoT devices, and they want greater information about how businesses gather and use their information. Experts also warn about IoT device security flaws [20], which might let an attacker to take control of a device or steal personal information. Insecure authentication techniques, transmission of unencrypted data, and failure to fix known defects are among the vulnerabilities. Furthermore, certain gadgets capture sensitive data and communicate it to the device manufacturer or other third parties, posing a privacy risk. Consumers are now unable to acquire information on device security and privacy before to purchase or at the time of purchase. The Mozilla "Privacy Not Included" purchasing guide website is an example of a resource for consumers seeking information on IoT device privacy and security [21]. It is not, however, designed as a label and is not tied to or linked to retail devices. Furthermore, when manufacturers withhold certain information, the product guide may be incomplete. Furthermore, as far as we are aware, the buyers guide has not been subjected to user testing.

Labels for IoT devices are being developed and used more often as a result of recent efforts. A government investigation in the United Kingdom, for example, advocated a voluntary labelling plan for IoT devices, and a collaboration of British institutions is working on a consumer security index for IoT devices. A number of bills related to IoT device privacy and security have been introduced in the United States. The Cyber Shield Act of 2017, for example, would provide an optional label for IoT devices that would include independent testing and cybersecurity compliance grades. The Internet of Things Cybersecurity Improvement Act of 2017 would force federal organisations to incorporate contractual conditions in IoT devices purchased by the US government that require security features.

Pre-Purchase Behavior

Curiosity was a major factor in IoT gadget purchases, particularly among owners of Intelligent Personal Assistants (IPAs) like Amazon Echo and Google Home. The desire to enhance one's health and fitness drove the majority of wearable purchasers. Other reasons highlighted by interviewers included cost and convenience. The majority of interviewees cited reliability issues and a lack of requirement as reasons for not purchasing smart home devices,

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106032 |

whereas price was cited as a factor for not purchasing wearables. Some respondents cited concerns about privacy and security as reasons for not buying a specific smart home product. Only a few people mentioned privacy concerns as a reason for not buying wearables. P6 stated that he did not purchase a smart door lock because he was concerned about its security of the device.

P7 also stated that she would not purchase Google Home because she was concerned that it would always listen to her.

Look and feel, customer service, prior experience with the device or similar devices, ease of use, reliability, opinion from experts (magazine reviews, electronics store employees), compatibility with other devices, durability, opinion from friends, opinion from family members, brand, privacy, security, customer reviews, price, and features were among the 16 factors mentioned by participants that influenced their purchase decisions. After price and features, interviewees identified privacy and security as the most relevant factors, according to the card sorting activity. Due to the small number of participants and the variability in the number of cards sorted by each participant, the card sorting activity should not be evaluated quantitatively. We conducted a large-scale survey to further investigate the relative influence of factors.

Post-Purchase Behavior

When we asked interviewees about their IoT device worries and challenges, the majority highlighted minor technical issues, with around half mentioning privacy or security concerns. The interviewer had not yet discussed privacy or security at this point in the conversation. Almost percent of the interviewees who expressed privacy issues were concerned about IPAs or smart TVs listening in on them. However, the majority of people who expressed security concerns had technical expertise and indicated mitigation measures such as attaching their IoT devices to a router that was separate from the rest of their home network.

IoT Device Privacy and Security

Interviewees were asked to define privacy and security in the context of IoT devices. Their definitions revealed that they had a limited understanding of privacy and security, with some unable to discriminate between the two.

The majority of participants defined privacy as having control over personal data when it comes to smart gadgets. "Privacy is whether it's up to me or them how they use my data," P16, for example, explained. Some discussed who data is shared with, while others discussed the types of data gathered, retention length, data collecting purpose, and inferred data.

When we asked interviewees to define IoT security, the majority of them indicated protection from illegal access ("being hacked"). Protective measures were mentioned by half of the interviewees. For example, some people stated password security and authentication, while others highlighted firewalls, encryption, and physical locks. Several people noted the dangers of illegal access to personal information.

Participants generally agreed that they should have control over their data when defining privacy. Except for individuals with technical backgrounds, who were more proactive in mitigating their security worries, they were generally passive when characterising security as the device being hacked. About half of our interviewees couldn't tell the difference between smart device privacy and security. Most interviewees who expressed pre-purchase or post-purchase privacy or security concerns, on the other hand, were better able to distinguish between the two. This shows that a lack of privacy or security concerns could be due to a lack of clear definitions for these two notions.

Purchase Behavior Categories

Our interview questions focused on five aspects of purchasing behaviour: risk awareness, privacy and security knowledge, pre-purchase privacy and security evaluation, post-purchase concern, and post-purchase worry management.

The majority of interviewees did not consider privacy or security before making their purchase, but were concerned about their device's privacy or security afterward. We discovered that hearing about issues from friends, media stories, and the item behaving in an unexpected way were the main causes of post-purchase worries. This was described as passive behaviour. Half of the interviewees who acted passively took some steps to deal with their worries (labeled as passive protective)."So in a movie, you know, some crazy hacker, they can get into all the films and cameras, so I know I put a sticker on my laptop camera, always," P1 said, "but I can't put a sticker on my home camera because I need to see what's happening, so I do worry about... my camera system being hacked."

Finally, during both the pre-purchase and post-purchase stages, a few of our interviewees stated that they were unconcerned with the privacy and security of their gadgets. We discovered two frequent reasons why people were unconcerned about the IoT devices they owned. They either did not consider the information acquired to be sensitive or indicated confidence in their ability to defend themselves from privacy and security issues. P9, for example, claimed she was unconcerned about her home security system because "you can't watch it online or even on the app unless the

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106032 |

phone is connected to the camera and you have a user name and password." "I have a passcode on it," remarked P21, another unconcerned interviewee. So I'm not worried about it being seen, and aside from my texts, I don't think there's anything I need to keep private." It's crucial to note that being unconcerned with IoT devices doesn't mean you don't care about privacy or security, as some of the indifferent interviewees said they would beconcerned if they owned other types of IoT devices.

V. CONCLUSION

Perceived quality is a key determinant of Indian customers' purchasing decisions for both Indian and local items, according to the study. The extent to which IoT devices provide security capabilities to safeguard consumers from internet risks varies greatly. Furthermore, it is currently difficult (if not impossible) for consumers to distinguish between devices that provide appropriate levels of security and those that do not at the time of purchase. This puts a stumbling block in the way of customers adopting purchasing habits that might help them build trust and protect themselves from cybercrime. We present a research of customer behaviour and purchase decisions in this paper. After doing research, it was discovered that IoT has security difficulties during the purchasing process. In the future, we must address this issue by adding security levels to each product, allowing consumers to browse the market and select the appropriate equipment.

REFERNCES

[1] Borhan. 2016. Perceived quality and emotional value that influence consumer's purchase intention towards American and local products. Procedia Economics and Finance 35 (2016), 639–643.
[2] RD Blackwell, PW Miniard, and JF Engell. 2006. Consumer Behaviour, 10th International Student ed. Thomson South-Western, Mason, OH (2006).
[3] Mesay Sata. 2013. Factors affecting consumer buying behavior of mobile phone devices. Mediterranean Journal of Social Sciences 4, 12 (2013), 103.
[4] Mary Catherine Gilly. 1980. Complaining Consumers: Their Satisfaction With Organizational Responses and Subsequent Credit Card Repurchase Behavior. (1980).
[5] Heikki Karjaluoto, Jari Karvonen, Manne Kesti, Timo Koivumäki, Marjukka Manninen, Jukka Pakola, Annu Ristola, and Jari Salo. 2005. Factors affecting consumer choice of mobile phones: Two studies from Finland. Journal of Euromarketing 14, 3 (2005), 59–82.
[6] Chen Ling, Wonil Hwang, and Gavriel Salvendy. 2006. Diversified users' satisfaction with advanced mobile phone features. Universal Access in the Information Society 5, 2 (2006), 239–249.
[7] Zoë Mack and Sarah Sharples. 2009. The importance of usability in product choice: A mobile phone case study. Ergonomics 52, 12 (2009), 1514–1528.
[8] Zhang, M.; Raghunathan, A.; Jha, N.K. Trustworthiness of medical devices and body area networks. Proc. IEEE 2014, 102, 1174–1188.
[9] Li, C.; Raghunathan, A.; Jha, N.K. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In Proceedings of the 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, HEALTHCOM 2011, Columbia, MO, USA, 13–15 June 2011; pp. 150–156.
[10] Harsh Pratap Singh, R. P. Singh, Rashmi Singh, and Bhaskar Singh, "Internet of Things (IoT) Based on User Command Analysis and Regulator Systems", International Conference on Recent Trends in IoT and Blockchain, 2019.
[11] Cherdantseva, Y.; Hilton, J. A Reference Model of Information Assurance & Security. In Proceedings of the 2013 International Conference on Availabil.
[12] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. 2017. Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic. arXiv preprint arXiv:1708.05044 (2017). [13] Jerry C Olson and Jacob Jacoby. 1972. Cue utilization in the quality perception process. ACR Special Volumes (1972).
[13] Todd Powers, Dorothy Advincula, Manila S Austin, Stacy Graiko, and Jasper Snyder. 2012. Digital and social media in the purchase decision process: A special report from the Advertising Research Foundation. Journal of advertising research 52, 4 (2012), 479–489.
[14] Cate Riegner. 2007. Word of mouth on the web: The impact of Web 2.0 on consumer purchase decisions. Journal of advertising research 47, 4 (2007), 436–447.
[15] Feng Zhu and Xiaoquan Zhang. 2010. Impact of online consumer reviews on sales: The moderating role of product and consumer characteristics. Journal of marketing 74, 2 (2010), 133–148.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106032 |

[16] Feng Zhu and Xiaoquan Zhang. 2010. Impact of online consumer reviews on sales: The moderating role of product and consumer characteristics. Journal of marketing 74, 2 (2010), 133–148.
[17] Janice Y Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. The effect of online privacy information on purchasing behavior: An experimental study. Information Systems Research 22, 2 (2011), 254–268.
[18] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 3393–3402.
[19] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. 2009. A nutrition label for privacy. In Proceedings of the 5th Symposium on Usable Privacy and Security. ACM, 4.
[20] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. 2015. Security, privacy and trust in Internet of Things: The road ahead. Computer networks 76 (2015), 146–164.
[21] Mozilla. 2018. Shop Safe This Holiday Season. https://foundation. mozilla.org/en/privacynotincluded/

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details