Lapai Journal of Science and Technology, Vol. 9, No. 1 (2023)

PRIVACY AND SECURITY CHALLENGES IN THE INTERNET OF THINGS: EMERGING TRENDS AND SOLUTIONS

***Bamanga, M. A., Dikko, E. S. and Shehu, M. A.**

*Computer Science Department, Federal University of Lafia, Nasarawa State
Corresponding e-mail: mahmud.bamanga@science.fulafia.edu.ng

ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices has ushered in numerous societal benefits but has also raised significant privacy and security concerns. This journal article delves into the pivotal role of IoT in society, the challenges confronting IoT privacy and security, threats and attacks targeting IoT devices, and the existing solutions and gaps in addressing these challenges. To achieve its objectives, the study formulated five research questions as guiding principles. A standard questionnaire served as the primary data collection tool, involving 100 IoT device users and a sample of 20 IoT industry stakeholders, encompassing developers, manufacturers, and policymakers. Data collection and analysis were conducted using SPSS version 26. The findings underscore a noteworthy consensus among both users and industry experts regarding the risks associated with data collection, authentication, firmware updates, network vulnerabilities, data integrity, and user awareness. These challenges bear substantial implications for user privacy and the overall security of IoT systems. Consequently, the study recommends the comprehensive integration of user education initiatives, user-friendly privacy solutions, a "privacy by design" ethos for developers, and public-private cooperation to enact practical and effective regulations. Through the adoption of these measures, stakeholders, policymakers, and industry participants can collaboratively enhance the security and privacy of IoT devices, fostering user trust and promoting the responsible adoption of IoT technologies. The study highlights the imperative for proactive measures to address these concerns, emphasizing the shared apprehension among stakeholders and users about the potential risks posed by IoT devices, along with the call for universally endorsed regulations or standards to safeguard privacy and security within IoT environments. This underscores the urgency of policy initiatives and educational campaigns to tackle these critical issues and reinforce the overall security and privacy of IoT ecosystems.

Keywords: Internet of Things (IoT), Privacy, Data privacy, Authentication, Firmware Updates, Data integrity

INTRODUCTION

The term "internet of things" (IoT) refers to the concept of numerous types of wired or wirelessly connected products and gadgets. IoT, or the internet of things, has grown in popularity due to its applications in communication, transportation, education, and corporate development, among others. Among others, Alferidah and Jhanjhi (2020). Inadvertent use, failure to change passwords, and failure to upgrade devices have all raised the probability of cyber-security breaches and the availability of key IoT system data to malevolent applications. Such lax security methods increase the likelihood of a data breach and other threats. The majority of security professionals see IoT as a point of risk for assaults due to low security standards and policies. Despite the fact that many security approaches have been developed to protect IoT devices from cyberattacks (Conti et al., 2018), security rules are not clearly established.

Furthermore, as IoT networks grow around the world, businesses will become concerned about the cross-linking of items. Because different devices have distinct characteristics, but they all share IoT, there will surely be new challenges to influence and exchange, which may pose dangers to the security of actual data or information, as well as the requirement for data protection for users. These aspects should be considered while establishing IoT infrastructure, and if they are not, there will surely be an imbalance in the adoption of IoT technology by enterprises, users, or other individuals using this technology (Salami et al., 2016).

Privacy and security concerns must be taken seriously, and IoT infrastructures must be appropriately secured to prevent security breaches. This is conceivable if designers and developers are properly led in integrating all security and privacy safeguards for IoT devices, causing customers to use the IoT infrastructure built into these devices automatically (Alferidah and Jhanjhi et al., 2020). The goal of this research is to identify, evaluate, and

offer viable solutions to privacy and security challenges that IoT networks and devices confront.

Aim and Objectives

The aim of this research is to identify and evaluate the privacy and security challenges facing IoT devices and network and provide effective solutions to address these challenges with the following objectives;

i. To identify the privacy and security challenges facing IoT devices and networks
ii. To examine the existing solutions to privacy and security challenges in IoT.
iii. To evaluate the effectiveness of the current solution to privacy and security challenges in IoT.
iv. To identify the gaps in current solutions and areas where further research is needed.
v. To provide recommendations for stockholders in IoT to enhance privacy and security.

Research Questions

i. What are the privacy and security challenges facing IoT devices and networks?
ii. What are the existing solutions to privacy and security challenges in IoT, and how effective are they?
iii. How effective are the current solutions in addressing privacy and security challenges in IoT, and what factors contribute to their success or failure?
iv. What are the gaps in the current solutions, and where further research is needed to address privacy and security challenges in IoT?

LITERATURE REVIEW

History of the internet of things and its Growth

The Internet of Things (IoT) is a very new concept that has just recently emerged. Kevin Ashton used the phrase "internet of things" for the very first time in 1999. After Ashton used it as the title of his presentation for a new sensor project he was working on (Aleisa and

Renaud, 2017), the word began to gain popularity among the general public. The very first device to be connected to the Internet of Things was developed at Carnegie Mellon University in the early 1980s. A group of students at the university came up with a way to enable the vending machine to report on its inventory to a network in order to spare themselves the inconvenience of having to drive off campus every time the Coca-Cola machine on campus ran out of drink. They attached microswitches to the gadget so that it could provide information regarding the availability of coke cans as well as their temperature.

In 1990, John Romkey was the first person to connect a toaster to the internet. One year later, many students from the University of Cambridge used a webcam to record coffee. They came up with the brilliant idea of employing the very first prototype of a web camera in order to keep track of how much coffee was still in the coffee maker located in the computer lab. They were successful in accomplishing this by configuring the web camera to take a photo of the coffee machine three times per minute. After that, the images were sent to neighbouring computers so that everyone could check to see if there was any coffee left (Liu, Xiao, and Chen, 2012). At this time, there are over 27 billion devices that are connected to the internet, but scientist's project that by the year 2030, there will be over 100 billion connected devices.

Importance of the Internet of Things to Society

i. The Internet of Things makes our surrounds smarter and more measurable, including our homes, businesses, and automobiles.
ii. It provides intelligent mobility solutions that optimise traffic flow, reduce fuel consumption, prioritise car repair schedules, and save lives.

iii. It enables the efficient linking of smart electric grids to renewable energy sources, hence improving system dependability and allowing users to be charged in smaller usage increments (Mwasilu et al., 2014).

iv. It enables machine monitoring sensors to detect and predict imminent maintenance issues, part shortages, and even prioritise maintenance personnel schedules for local needs and repair equipment.

v. The infrastructure of "smart cities" is being built using data-driven systems, making it easier for local governments to manage garbage, law enforcement, and other activities more successfully.

IoT privacy and security challenges

IoT has provided users with numerous benefits; nevertheless, it has also presented certain drawbacks. Among these difficulties are:

i. IoT devices are linked together in order to communicate and exchange data. This jeopardises both user privacy and data security. It is vital in IoT circumstances to protect user data and ensure their privacy. Data management, sharing, management, and security are important themes and ongoing research areas (Obaidat, et al., 2020).

ii. Identity and authentication management: Management, protecting object profiles, and guaranteeing safe data and resource access are all critical considerations in the Internet of Things. These considerations are made possible by combining identity management and authentication techniques. Identity management techniques are used to uniquely identify items in the IoT environment, whilst authentication techniques are used to protect and authenticate the identity establishing between objects. (Obaidat, et al., 2020).

iii. Policy integration and trust management The IoT environment is perplexing. In this disturbing environment, trust is required for object-to-object communication. In the

untrustworthy IoT context, trust must be considered in order to establish secure connection. The two viewpoints on trust in the IoT are user trust and trust among communicating IoT gadgets. (Obaidat, et al., 2020).

iv. Authorization and access control: After gaining access to the IoT network via user authentication, users must be authorised to determine whether they or other objects have access to the network's resources. Access control refers to the process of regulating resource access. The use of access control results in authorization. To establish a secure connection between services and objects, authorisation and access control mechanisms must be used. Authentication plays a significant role in confirming users' identities by matching database information with user credentials. End-to-end security for the Internet of Things: End-to-end security in IoT assures that both parties interact on the basis that no one can spy on their connection since their communication is secure and hidden from everyone, and attackers cannot change the sent data. Endpoint security is critical when connecting internet hosts and IoT devices. Encryption and authentication via packet codes are insufficient to ensure complete end-to-end IoT security. In order to validate end-to-end security on both communicating ends, algorithms and protocols must be considered in addition to achieving individuality verification. (Obaidat, et al., 2020).

v. Security solution that is resistant to attacks: IoT devices exist in a wide range of shapes and sizes, with various amounts of memory and computational power. The devices involved are vulnerable to attacks. As a result, security countermeasures and attack resistance solutions should be easily available. (Obaidat, et al., 2020).

Threat and Attacks to IoT Devices

Because IoT devices are designed to fulfil the general needs of an organisation and an individual, they lack adequate security standards. Attackers have used this advantage to get access to a company's system via any unprotected IoT device.

IoT assaults are cyberattacks that use any IoT device to gain sensitive consumer data. Attackers generally cause device damage, install malware on it, or get access to more personal information belonging to a company or an individual.

According to (office of information security securing one HHS, health sector cyber security coordination center, 2020) stated that some of these attacks includes:

i. Privilege Escalation: By taking advantage of bugs, unpatched vulnerabilities, design flaws, or even operating systems, an attacker can gain unauthorised access to an IoT device.
ii. Man-in-the-middle (MITM) attacks are a subset of denial-of-service attacks in which a third party intercepts data being transmitted between two parties. Information can potentially be stolen or altered using this technique.
iii. Eavesdropping is the act of an attacker intercepting, erasing, or changing data passed between devices. This attack makes use of unreliable network connections.
iv. Brute-force attacks: Many Internet of Things (IoT) devices come with pre-configured passwords that are not changed. Threat actors may employ brute force attacks to get access.
v. Each gadget has software, updates, and changes. v. Firmware Hijacking. By installing fake updates or drivers that trigger the installation of malicious software, actors can profit from this environment.
vi. Distributed denial of service (DDOS): IoT devices can be abused to conduct significant cyberattacks when they are infected with botnet malware.

vii. Physical Tampering: To install malware on vulnerable IoT devices, threat actors may get access to the devices first.

Table 1: Existing Solutions to Privacy and Security Challenges in IoT and there Gaps

Author name	Proposed solution	Research gap
Lewis *et al.* (2023)	To conduct a survey that summarizes state-of-the-art "Access Control" techniques and technologies. This survey aims to present recent research trends in the field of Access Control and also discuss the adoption and application of these techniques in various domains such as Cloud Computing, Blockchain, the Internet of Things, and Software-Defined Networking.	There is need for comprehensive survey of Access Control techniques and technologies, especially in the context of emerging technologies and evolving cybersecurity threats.
Whyte, Omoyiola, and Okoni (2022).	The use of blockchain technology to provide data integrity assurance. It highlights the high-level security capabilities of blockchain technology, including cryptography encryption, which is intended to protect data from attackers, prevent fraud and manipulation, and reduce the risk of data theft or compromise. The proposed solution aims to ensure data integrity, confidentiality, availability, security, efficiency, and user privacy by leveraging blockchain technology.	Blockchain security and data integrity assurance applications need to be addressed.
Rashid et al. (2021)	The development of an intrusion detection system (IDS) is using a combination of deep learning approaches (CNN, RNN, and LSTM) and traditional machine learning algorithms (SVM, Random Forest, and XGBoost).	The need for effective intrusion detection systems specifically designed for wireless networks.
Obaidat et al. (2020)	Security policy based on the Seckit concept and combined with the MQTT protocol layer to increase the security and privacy of IoT devices	Limited because of its battery constraints

Tao and Peiran (2010)	a preference-based privacy protection mechanism for IoT	The protection mechanism is not developed enough to hold privacy.
Ali et al. (2019)	Network design for smart home gateways based on blockchains for decentralisation and security risk control.	The gateway has a single point of failure vulnerability.
Pierre de Leusse. (2012)	Self-managed security cells (SMSC) is a scalable approach for enhancing distributed resource security.	It currently does not validate for specific applications or security purposes.
Aleisa (2017)	Authentication and access control mechanism for IoT devices to close security gaps and ensure data integrity.	Man-in-the-middle assault, eavesdropping attack
Alhalafi and Veeraraghavan (2019)	the use of PUF (physical untouchable functions) to provide device authentication	its requires a lot of computing power to authenticate all the objects message and device in a given IoT network
Chen *et al.* (2006)	An algorithm for detecting defective sensors in WSNS. This algorithm demonstrates that it can accurately identify malfunctioning sensors.	Forgery attack, location privacy issue, and replay attack are all possible.
Salami *et al.* (2016)	A lightweight identity-based encryption system designed specifically for smart homes.	Overhead of handling private key generator.
Raza *et al*. (2011)	End-to-end security technique for internet and IP sensor network connection.	The network is prone to dos attack

METHODOLOGY

Research Design

The research design will include both qualitative and quantitative data collection methods, which will allow for a comprehensive analysis of the research questions and objectives. Interviews with important stakeholders in a semi-structured manner will be one of the qualitative data collection techniques in the IoT industry, including developers, manufacturers, and policymakers. The interviews will explore the privacy and security

challenges facing IoT devices and networks, the effectiveness of existing solutions, and the recommendations for enhancing privacy and security (Ali et al., 2019).

The quantitative data collection methods will include a survey of end-users to gather their perspectives on privacy and security challenges in IoT devices and networks, their knowledge of existing solutions, and their willingness to adopt best practices for enhancing their privacy and security. The research design will also include a review of existing literature on privacy and security challenges in IoT devices and networks and the effectiveness of existing solutions. The literature review will help to identify the gaps in the current knowledge and provide a foundation for the research questions and objectives. The data collected through interviews, surveys, and literature review will be analysed using a thematic analysis approach. This method will make it possible to find patterns and themes in the data, which will provide us insights on the privacy and security issues that face IoT networks and devices as well as the efficacy of current solutions.

Population and Sample Size of the Research

The primary method employed for data collecting involved the utilization of a standardized questionnaire. This instrument was administered to a total of 100 individuals who were users of IoT devices. Additionally, a subset of 20 individuals representing stakeholders within the IoT industry, including developers, manufacturers, and policy makers, were also surveyed using the same questionnaire.

Data Collection Methods

Several techniques will be used for the study's data collection, including:

i. **Semi-structured interviews**: this method will be used to collect qualitative data from key stakeholders in the IoT industry, including developers, manufacturers, and policymakers. The interviews will be conducted in-person, over the phone, or through video conferencing platforms, and will follow a semi-structured format,

allowing for open-ended responses and follow-up questions. The interviews will explore the privacy and security challenges facing IoT devices and networks, the effectiveness of existing solutions, and the recommendations for enhancing privacy and security.

ii. **Surveys:** a survey will be used to collect quantitative data from end-users of IoT devices and networks. The survey will be administered online, and will include questions on the privacy and security challenges facing end-users, their knowledge of existing solutions, and their willingness to adopt best practices for enhancing their privacy and security.

iii. **Literature review:** a comprehensive literature review will be conducted to gather existing information on privacy and security challenges in IoT devices and networks and the effectiveness of existing solutions. This will be done through a systematic search of academic databases and other relevant sources.

iv. **Observations:** observations will be conducted to gather additional information on how end-users interact with IoT devices and networks. This will help to identify potential privacy and security challenges that may not be captured through interviews or surveys.

Data Analysis Techniques

Data validation is a critical step in ensuring that the data collected for the study on "IoT privacy and security challenges and solution" is accurate, reliable, and trustworthy. The following techniques will be used to validate the data collected:

i. **Triangulation**: triangulation involves using multiple data sources to confirm or validate the findings of the study. In this study, the data collected through semi-structured interviews, surveys, literature review, and observations will be triangulated to validate the results.

ii. **Member checking:** Member checking entails informing participants of the research findings to confirm that the results accurately reflect their experiences and perspectives. In this study, the results of the semi-structured interviews will be presented to the key stakeholders in the IoT industry for member checking.

iii. **Peer debriefing:** To get feedback and new perspectives, peer debriefing entails discussing research findings with other scholars working in the same area. In this study, the research findings will be shared with other researchers in the field of IoT and cyber security for peer debriefing.

iv. **Data cleaning**: data cleaning involves reviewing the collected data to identify and correct any errors or inconsistencies. In this study, the collected data will be thoroughly reviewed to ensure accuracy and completeness.

v. **Statistical analysis**: statistical analysis involves using appropriate statistical techniques to analyse the quantitative data collected through the survey. This will help to validate the findings and draw meaningful conclusions.

Validity and Reliability of the Research Instruments

Validity and reliability are crucial components of every research study, including the one on "privacy and security challenges in IoT and solutions." To assure the study's validity and reliability, the following steps will be taken:

i. **Construct validity**: to ensure construct validity, the study was used a number of data collection approaches, such as semi-structured interviews, surveys, and questionnaires literature review, and observations. These allowed for triangulation of data sources and provide a comprehensive understanding of the research topic.

ii. **Internal validity**: internal validity was used to ensure by using appropriate sampling techniques to select participants for the study. The study also used standardized protocols for data collection and analysis to minimize the risk of bias and ensure the internal validity of the instruments.

iii. **External validity:** to ensure external validity, the study used a representative sample of end-users and key stakeholders in the IoT industry. This was enabled the study findings to be generalized to the broader population of IoT users and stakeholders.

iv. **Reliability**: reliability was adopted to ensure standardized data collection protocols, training data collectors to follow the protocols consistently, and using appropriate statistical techniques for data analysis. The study was also conduct member checking and peer debriefing to ensure the reliability of the study findings.

v. **Data analysis**: the data analysis process was transparent, systematic, and rigorous. The study used appropriate statistical techniques to analyse the quantitative data collected through the survey. The qualitative data collected through semi-structured interviews, literature review, and observations was analysed using thematic analysis.

PRESENTATION OF FINDINGS

Analyses of the Results

The data for this research work were obtained using primary source of data was collected and analysed with the statistical programme for social sciences (SPSS) version 26. A questionnaire was distributed to IoT stake-holders and users, where 15 questionnaires were retrieved from 20 questionnaires given to the stake-holders while 70 out of 100 questionnaires were also retrieved from IoT users.

Table 2: Response rate for stake-holders: Age

Respondents	Frequency	percent	valid percent	cumulative percent
under 18yrs	1	6.7	6.7	6.7
18-24	4	26.7	26.7	33.3
25-34	10	66.7	66.7	100.0
Total	15	100.0	100.0	

The above table shows that out of 15 respondents, 66.7% of them were from 25-34yrs age group, 26.7% were from age group 18-24 while 6.7% of the respondents were under 18yrs.

Table 3: Distribution of Response by Gender

Respondents	Frequency	Percent	valid percent	cumulative percent
Male	12	80.0	80.0	80.0
Female	3	20.0	20.0	100.0
Total	15	100.0	100.0	

The response from the survey also shows that 80% of the stake-holders were male while 20% were female.

Table 4: Distribution of Reference by Occupation: Occupation

Respondents	frequency	Percent	valid percent	cumulative percent
Student	9	60.0	60.0	60.0
self-employed	6	40.0	40.0	100.0
Total	15	100.0	100.0	

The table above shows that 40% of the stake-holders were self-employed while 60% of them were students.

Table 5: Distribution of Response by Education: Education

Respondents	Frequency	percent	valid percent	cumulative percent
SSCE	1	6.7	6.7	6.7
NCE/ND	6	40.0	40.0	46.7
Bsc	5	33.3	33.3	80.0
MSc	3	20.0	20.0	100.0
Total	15	100.0	100.0	

From the response above 20% of the stake-holders were attained master degree, 33.3% of them attained Bachelor of Science, 40 % attained NCE/ND while 6.7% attained SSCE

Table 6: Distribution of Response by Perception of privacy and security challenges in IoT: Do you believe that internet of things (IoT) pose a risk to privacy and security?

Respondents	Frequency	Percent	valid percent	cumulative percent
Yes	11	73.3	73.3	73.3
No	4	26.7	26.7	100.0
Total	15	100.0	100.0	

From the table above 73.3% of the respondents agreed that IoT pose a risk to privacy and security while 26.7% disagreed.

Table 7: Distribution of Response by Experience

Respondents	Frequency	Percent	valid percent	cumulative percent
Yes	8	53.3	53.3	53.3
No	7	46.7	46.7	100.0
Total	15	100.0	100.0	

The table shows that 53.3% of the respondents did not experience any security breaches while using IoT devices while 46.7% of them experienced privacy and security breaches by using IoT device.

Table 8: Distribution of Response by Awareness of any measures to protect privacy and security while using IoT devices: Are you aware of any measures to protect privacy and security while using IoT devices?

Respondents	Frequency	Percent	valid percent	cumulative percent
Yes	7	46.7	46.7	46.7
No	8	53.3	53.3	100.0
Total	15	100.0	100.0	

The response above indicates that 53.3% of the respondents are not aware of the measures to take to protect their privacy and security while using IoT while 46.7% of them are aware.

Table 9: Distribution of Response by Perception of privacy and security: Do you feel comfortable sharing personal information with IoT devices?

Respondents	Frequency	percent	valid percent	cumulative percent
Yes	2	13.3	13.3	13.3
No	13	86.7	86.7	100.0
Total	15	100.0	100.0	

The result above shows that 86.7% of the respondents are not comfortable sharing personal information with IoT devices while 13.3% of the respondents are comfortable.

Table 10: Distribution of Response by how much do you value your privacy: How much do you value your privacy and security while using IoT devices?

Respondents	**Frequency**	**percent**	**valid percent**	**cumulative percent**
Low	1	6.7	6.7	6.7
moderate	3	20.0	20.0	26.7
High	11	73.3	73.3	100.0
Total	15	100.0	100.0	

The table above indicates that 73.3% of the respondents highly value their privacy and security while using IoT devices while 20% of them moderately care on their privacy while using IoT devices

Table 11: Distribution of Response by Experiences while using IoT devices: Have you experienced any negative consequences as a result of using IoT devices?

Respondents	**frequency**	**Percent**	**valid percent**	**cumulative percent**
yes	5	33.3	33.3	33.3
No	10	66.7	66.7	100.0
total	15	100.0	100.0	

The result of the survey also shows that 66.7% of the stake-holders had experienced negative consequences as a result of IoT devices while 33.3% had no negative experienced while using IoT devices

Table 12: Distribution of Response by Have you used any privacy and security solution for IoT devices: Have you used any privacy and security solutions for IoT devices?

Respondents		**frequency**	**Percent**	**valid percent**	**cumulative percent**
Valid	yes	8	53.3	53.3	53.3
	No	7	46.7	46.7	100.0
	Total	15	100.0	100.0	

The table above indicates that 53.3% of the respondents once used privacy and security solution for IoT devices while 46.7% of them did not use that.

Table 13: Distribution of Response of stakeholders by how effective is the existing solution: How effective do you think these solutions are in protecting privacy and security in IoT devices?

Respondents	frequency	percent	valid percent	cumulative percent
Less effective	4	26.7	26.7	26.7
Moderate	5	33.3	33.3	60.0
Very effective	6	40.0	40.0	100.0
Total	15	100.0	100.0	

The result of the survey indicates that 40% of the stake-holders rate solution to IoT devices very effective, 33.3% of them considers it moderate while 26.7% consider it less effective.

Table 14: Do you think there should be regulations or standards in place to protect privacy and security in IoT devices?

Respondents	frequency	percent	valid percent	cumulative percent
Yes	15	100.0	100.0	100.0

From the response above all the stake-holders agreed that a standard regulation should be put in place in other to privacy and security in IoT devices.

Table 15: Response rate for IoT users for age: Response rate for IoT users

Respondents	frequency	percent	valid percent	cumulative percent
18-24	43	61.4	61.4	61.4
25-34	23	32.9	32.9	94.3
35-44	4	5.7	5.7	100.0
Total	70	100.0	100.0	

The above table shows that out of 70 respondents, 61.4% of them were from age group 18-24yrs, 32.9% were from age group 25-34 years while 5.7% of the respondents were from age group 35-44yrs.

Table 16: Response rate for IoT users for Gender

Respondents	Frequency	percent	valid percent	cumulative percent
Male	44	62.9	62.9	62.9
female	26	37.1	37.1	100.0
Total	70	100.0	100.0	

The response from the survey shows that 62.9% of the IoT users were male while 37.1% were female.

Table 17: Response rate for IoT users for Education: Education

Respondents	frequency	percent	valid percent	cumulative percent
SSCE	7	10.0	10.0	10.0
NCE/ND	8	11.4	11.4	21.4
Bsc	52	74.3	74.3	95.7
MSc	3	4.3	4.3	100.0
Total	70	100.0	100.0	

From the response above 74.3% of the respondents attained Bsc, 11.4% of them attained NCE/ND, 10.0% attained SSCE while only 4.3% attained MSc.

Table 18: Response rate for IoT users for Occupation: Occupation

Respondents	Frequency	percent	valid percent	cumulative percent
Student	49	70.0	70.0	70.0
self-employed	20	28.6	28.6	98.6
employed part-time	1	1.4	1.4	100.0
Total	70	100.0	100.0	

The table above shows that 70% of the respondents are students, 28.6% are self-workers while 1.4% of them are employed but part-time.

Table 19: Response rate for IoT user Perception of privacy and security challenges in IoT: Do you believe that internet of things (IoT) pose a risk to privacy and security?

Respondents	frequency	percent	valid percent	cumulative percent
Yes	42	60.0	60.0	60.0
No	28	40.0	40.0	100.0
Total	70	100.0	100.0	

From the table above 60% of the respondents agreed that IoT pose a risk to privacy and security while 40% disagreed.

Table 20: Response rate for IoT users for have you experience any privacy or security breach in using IoT device: Have you experience any privacy or security breaches in using IoT devices?

Respondents	Frequency	percent	valid percent	cumulative percent
Yes	30	42.9	42.9	42.9
No	40	57.1	57.1	100.0
Total	70	100.0	100.0	

The table shows that 57.1% of the respondents did not experienced any security breaches while using IoT devices while 42.9% of them experienced privacy and security breaches by using IoT device.

Table 21: Response rate for IoT users for awareness of any measures to protect privacy and security while using IoT devices: Are you aware of any measures to protect privacy and security while using IoT devices?

Respondents	Frequency	Percent	valid percent	cumulative percent
Yes	43	61.4	61.4	61.4
No	27	38.6	38.6	100.0
Total	70	100.0	100.0	

The response above indicates that 38.6% of the respondents do not know the measures to take to protect their privacy and security while using IoT while 61.4% of them know

Table 22: Response rate for IoT users for factors affecting privacy and security concerns in IoT: How much do you value your privacy and security while using IoT devices?

Respondents	Frequency	percent	valid percent	cumulative percent
Low	4	5.7	5.7	5.7
Moderate	24	34.3	34.3	40.0
High	42	60.0	60.0	100.0
Total	70	100.0	100.0	

The table above indicates that 60% of the respondents highly value their privacy and security while using IoT devices while 34.3% of them moderately care on their privacy while using IoT devices, while 5.7% of they doesn't care.

DISCUSSION OF RESULTS

From the research question one "What are the demographics of IoT stakeholders and users?" the results show that stakeholders are primarily in the age group of 25-34, with the majority being male and consisting of both students and self-employed individuals. Education levels vary, with a significant percentage holding a Bachelor's degree. On the other hand, IoT users are predominantly in the 18-24 age group, mostly male, and primarily students with Bachelor's degrees.

And research question two "What are the perceptions of privacy and security challenges in IoT among stakeholders and users?" shows that both stakeholders and users express concerns about the privacy and security challenges in IoT. A majority of both groups believe that IoT poses a risk to privacy and security. Additionally, most stakeholders are uncomfortable sharing personal information with IoT devices, while IoT users highly value their privacy and security.

While the majority of stakeholders did not experience security breaches, a significant percentage of IoT users did. This indicates that there is a difference in the experiences of these two groups, with IoT users facing more privacy and security challenges from the

research question three "What experiences have stakeholders and users had with privacy and security brea*ches in IoT?"

Also, research question four "Are stakeholders and users aware of measures to protect their privacy and security while using IoT devices?" shows that awareness of security measures varies among stakeholders and users. A majority of stakeholders are aware of measures to protect their privacy and security, whereas a significant percentage of IoT users are not aware of such measures. This suggests that there may be a need for increased education and awareness among IoT users.

A substantial percentage of stakeholders have used privacy and security solutions for IoT devices, and a significant portion finds these solutions very effective. This indicates that stakeholders are proactive in addressing privacy and security concerns. However, IoT users are somewhat less likely to use such solutions, with a slight majority having used them from research question five "Do stakeholders and users use privacy and security solutions for IoT devices, and how effective do they find these solutions?"

Finally, the research question six "Do stakeholders and users believe that regulations or standards should be in place to protect privacy and security in IoT devices?" indicate that both stakeholders and users strongly support the idea of regulations or standards to protect privacy and security in IoT devices. All stakeholders and a majority of users believe such regulations are necessary, indicating a consensus on this issue.

CONCLUSION

The internet of things (IoT) has brought about many benefits, but it has also brought about new challenges related to privacy and security. As IoT devices become more prevalent in our daily lives, it is essential to address these challenges to ensure that users' privacy is protected and that their data is secure.

One of the biggest challenges with IoT devices is that they collect and transmit vast amounts of data, often without the user's knowledge or consent. This data can be sensitive, such as personal information, health data, or financial information. To address this challenge, IoT device manufacturers and service providers should implement strong privacy policies, use secure data encryption, and give users control over their data. Another challenge with IoT devices is that they are often vulnerable to cyber- attacks. Hackers can exploit vulnerabilities in IoT devices to gain access to sensitive data or even control the devices themselves. To address this challenge, IoT device manufacturers should prioritize security and implement secure coding practices, including regular updates and patches. Users should also take steps to protect their devices, such as using strong passwords, regularly updating firmware, and avoiding connecting to public Wi-Fi networks.

Overall, privacy and security challenges in IoT can be addressed through a combination of technological solutions and user education. As IoT continues to grow and evolve, it is essential to prioritize privacy and security to ensure that users can trust and benefit from these technologies.

REFERENCES

Alferidah, K. D. & Jhanjhi, N. Z. (2020). A review on security and privacy issues and challenges in internet of things. *International Journal of Computer science and network security*, Volume 20 (4).

Ali, J., Khalid, S. A., Yafi, E., Musa, S. & Ahmed, W. (2019). Towards a secure behaviour modeling for IoT network using block-chain, Madrid, Spain. Conferences workshop at the second International Conferences on applied information.

Conti, M., Dehghantanha, A., Franke, K. & Watson, S. (2018). Internet of things security and forensics: challenges and opportunities. *Future generation computing system*. 2018, 78, 544–546.

Health sector cyber security coordination center, office of information security securing one hhs. (August 4, 2020*). Internet of things IoT security*.

Lewis, G., Paolo, M., Rémi G. and Victor, C. (2023). Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN. *Cyber Security and Applications*. Volume 1, 2023. ISSN 2772-9184.

Liu, J., Xiao, V. & Chen, C. I. P. (2012) Authentication and Access Control in the Internet of Things. *32nd International Conference on Distributed Computing systems workshop*s, Macau, china, June 2012, p.588-592

Obaidat, M. A., Obeidat, S., Holst, J., Al Hayajneh, A., & Brown, J. A. (2020). Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. *Computers.* Volume 9(44).

Pierre de leusse, P. P. (2012). Self-managed security cell, a security model for the internet of things and services. *1st international conference on advances in future internet.* (pp. 47- 52). Athens.

Rashid, B., Artykbayev, K., Adam, K. & Mels, B. (2021). Intrusion Detection System for Wireless Networks. 16th International Conference on Electronics Computer and Computation (ICECCO), *Kaskelen, Kazakhstan*, 2021, pp. 1-5, doi: 10.1109/ICECCO53203.2021.9663787

Raza, S., Duquennoy, S., Chung, A., Yazar, D., Voigt, T. & Roedig, U. (2011, 27-29 June). Securing communication in 6lowpan compressed Ipsec. Distributed Computing In Sensor Systems. Barcelona Spain. *IEEE International Conference and Workshop*.

Salami, S. A., Baek, J., Salah, K. & Damiani, E. (2016). Lightweight Encryption for Smart Home. *11th international conference on availability, reliability and security*. IEEE.

Tao, H., & Peiran, W. (2010). Preference-Based Privacy Protection Mechanism for the Internet of Things. *3rd International Symposium on Information Science and Engineering*. Shanghai, China, December. 2010, p. 531-534, doi:10.1109/isise.2010.135.

Whyte, S. T., Omoyiola, B. O. & Okoni, B. E. (2022). Use of Blockchain Technology in Data Integrity Assurance. Available at SSRN: https://ssrn.com/abstract=4043164 or http://dx.doi.org/10.2139/ssrn.4043164