International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-11 Issue-11, October 2022

Critical Analysis of Data Privacy and Security on IoT Devices in An Organization

Ikechukwu Jonathan Ezea, Christiana Uchenna Ezeanya

Abstract*: *Everyone is trying to catch up with the changing technology world of our time. Every object has been computerized to achieve precision and accuracy in service delivery, reduce cost and eliminate error or reduced it to the barest minimum. The advent of telecommunication and inroad into the computer world has opened the space to get every object behave on predefined set of rules. Items ranging from household object to service and manufacturing material have all been programmed to understand and act digitally. The paper x-rayed the uses, challenges and breaches caused by IoT devicesin organizations. This paper took a critical study of the data privacy and security as it relates to IoT devices in an organization. It also enlightens users on the breaches caused by these devices and dangers of these breach on the organizational data security. In order to build a trust in the system, the researcher proffered ways of securing data in IoT devices in organizations to achieve maximum and needed security.

Keywords:* *Data, Information, IoT, Privacy, Security

I. INTRODUCTION

Today, data is the next goldmine. Data are ingredients for information. This simply means that we process and refine data to get information. Data Privacy is the act of keeping data in such a way that an unauthorized person will not have access to it. It is about storing data so that people who don't need it will not access it. Such information could be personal information like health or medical record, financial records, legal or other kinds of data. IoT which is the short form for Internet of Things is simply an aggregation or connection of billions of physical devices to the internet. Today little items as small as light bulbs, wrist watches and other small items are today controlled by internet application. Today, it is not unusual to see chairs, car and objects as big as airplanes that are being controlled by chips. The information about the operational and functionality of these devices have to be secure and as such they need to be private. The IoT devices will be vulnerable if the data or information about the functionality and operational models are not protected. For data to be private, it must be protected.

Manuscript received on 13 September 2022 | Revised Manuscript received on 20 September 2022 | Manuscript Accepted on 15 October 2022 | Manuscript published on 30 October 2022.

*Correspondence Author (s)
Ikechukwu Jonathan Ezea*, Department of Computer Science, Ebonyi State University, Abakaliki Nigeria. E-mail: iykeezea@gmail.com
Christiana Uchenna Ezeanya, Department of Computer Science, Ebonyi State University, Abakaliki Nigeria. E-mail: emmanuelchristy414@gmail.com

Therefore, data privacy and security seem to be the same. Data privacy is ensuring that data remains in the hands of who should have it while data security is a deliberate policy to protect data from an unauthorized user. When data is not secured and it gets into the hand of an unauthorized user especially in big organization, privacy is breached. Data privacy defines who has access to data, while data security provides protection to data using defined tools and policies to actually restrict access to the data. Imagine that the access to an IoT cabinet was modified by an unauthorized person giving access to private, confidential and secret files which can cause havoc to the organization. This can also be said of a door that the data manipulation was accessed and opened to invaders and robbers. Imagine a security manipulation as an IoT control switch, this simply means that even when the bulbs and all sockets in an organization are switched off, a security guard will have access to some sockets where he irons his clothes in the night thereby increasing the electricity charges for the organization. According to [1] NDPR provides legal safeguards for the processing of personal data. Under the NDPR, personal data must be processed in accordance with a specific, legitimate and lawful purpose consented to by the Data Subject. The act provides for personal data to be protected by organizations and could only be released to an authorized person. According to several authors, information security has become highly relevant and necessary for the survival of organizations [2][3]

II. REVIEW OF RELATED LITERATURE

A. Data Privacy Right

According to The [4] the following are the rights of the individual in data privacy.

- The Right to be informed: Your personal data is your personal property and cannot be collected or used by another other party without your prior consent
- The Right to Access: A data owner has the right to access or request to access to know who and who had access to his or her data, what they used it for and how they processed the data.
- The right to object: You have the right to object to a request for your information especially when you are not sure of what the information is requested for or would be used for.
- The right to erasure or blocking: An individual has the right to erase or block the data concerning him when the data are no longer needed for the purpose, or when it may be prejudicial or inaccurate, or when one thinks that such information could be dangerous or even when one thinks that the processing was unlawful.

- The right to damages: An individual can claim damages if he or she feels that an information used is false or outdated or obtained without prior consent.
- The right to file a complaint: When an individual feels that his or her data have been misused or obtained illegally, he or she can file a complaint in a court of law.
- The right to rectify: If the data by a personal information controller PIC holds about an individual is false, such individual has the right to rectify such an inaccurate data
- The right to data portability: Data portability confers the right to an individual to carry or move ones data to a more secured environment.

B. Data Breaches in IoT

According [5] Security Magazine (2022 that exposed over 22 billion records in 2021, approximately 5% fewer than in 2020. There are three ways data can be breached, they are according [6]

- Physical Breaches: This isnormally the kind of data breaches that occur when an employee is compromised or compromises his work tools such as laptops, desktops, hard drives, flash drives and any other data storage devices. This kind of breach can occur purposely when an employee or insiders steals data and hands such over to an authorized person. It can also occur when an organization inadvertently disposes an electronic storage device that exposes individual data. This has led to collapse of many organizations where the data exposed were used to get undue advantage against the organization by a competitor.
- Electronic Breaches: These breaches are deliberate unauthorized access into a website, or systems or networks of a particular organization by hackers. According [7]in Techack,in 2020a Nigerian student hacked into one of the second generation banks data base in Nigeria and exposed all the customers' records. This occurred because the attacker gained unlawful access into the banks data base. Although no harm was done financially but it caused panic in the system that could lead to mistrust by customers. According [8], a Nigeria bank lost 1.87b to a hacker due to unlawful access.
- Skimming: This has become a new way of data breaching. The process involves putting a device called skimmer into the card readers of ATMs or POS to capture vital data on the customers cards. This skimmer captures these data and exposes them to unauthorized individuals who use them to wreak havoc into the financial system or personal things.

C. Organizational challenges in applying security in IoT

IoT being a new technology allows the interconnection of several devices either physically or in virtual form. The operations of these devices are based on sensors that help in monitoring, controlling, and interacting with the physical environment where they exist. These devices which are difficult to control by the organization connects to the organizational network and poses so many risk.[9]stated that the authentication ofIoT devices is a great challenge due to its heterogonous and interconnected protocols. When IoT devices are connected, they generate data that are both personal and organizational data thereby sharing it with any other website it is connected to. [10] state that data security and privacy are joint issues that is associated with internet connectivity around the world. When these sensitive data are exposed to threats, it poses great challenge to the organization. Also monitoring, filtering, and blocking these malicious activities becomes a huge challenge to deal with. IoT devices generate a huge amount of data when connected to a network, and managing this data is also a challenge faced. [11] stated the following as the challenges that are associated with the security of the IoT devices in the organization

- Software and Firmware Vulnerabilities: It states that because some IoT devices are resource-constrained and have limited computing power, it makes the security of these devices difficult and the device becomes vulnerable. Some of these devices have poor access control and lack regular updates and patches that will fix vulnerabilities due to technical limitations. Even those that have updates, some users don't care to do that.
- Insecure communication: Most of the security mechanisms we have right now are designed to take care of desktop computers and are initiated during the design process, because of this, some security mechanisms are not applied to IoT devices. Due to this, connected devices are susceptible to attacks from other devices. When these devices are connected to the organizational network, the attacker might penetrate the organization network through the IoT devices.
- The third challenge is the data leakage associated with IoT devices. Hackers gain access to organizational networks by capturing unencrypted messages in IoT devices. These data include sensitive data like bank details and the location of the user. Sensitive data can also be gotten from third-party services, and cloud-hosted services once there is poorly secured communication
- Malware risks:-. Once an attacker succeeds in changing the functionality of an IoT system through the injection of malware, organizations are posed at risk. Due to inadequate software security of some IoT devices, these devices are easily penetrated and attacked. The inadequate software security creates a weakness in the IoT systems which the attackers leverage to exploit and abuse the network.
- Cyber-attack: Apart from the malware attack and other and other challenges listed above, IoT devices are also susceptible to cyber-attacks. Also because of the limited processing speed of the IoT devices, the network is vulnerable to DoS attacks and DoSL attacks. In DoSL attack, the attacker explores the vulnerabilities of the media access control protocol to initiate the DoSl. Other attacks associated with IoT are device spoofing which occurs when devices have improperly implemented digital signatures and encryption. Also if the device is stolen, attackers can tamper with the device to make them function in an unintended way.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

These challenges listed above are faced every day in an organization that allows the interconnection of IoT devices to its network

D. Importance of IoT security

Why is IoT security important in an organization? We know that IoT devices are disrupting consumers, enterprises, and government, and it's paving the way for the analytical revolution. Right now, there are lots of devices that are connected to the internet and the biggest question remains "Can technology company be able to secure all these devices from the threats" Securing the IoT devices cannot be overemphasized because if the devices are secured, the organization integrity and reputation are secured. How do we secure these devices in the network? For IoT devices to work efficiently, the hardware, software, and connectivity have to be secure. Without efficient security, any of these devices can be a threat vector where threats gain access to the network.

E. Ways of Resolving IoT security issues

[12] listed 3 ways IoT devices can be secured by tech professionals: First is by adopting security by design, the high tech companies should implement security of these devices at the design level. Implementing security in the design process will curb some security challenges associated with the devices. Secondly, the manufacturers of these IoT devices should employ different approaches to data security that is providing ways of ensuring that the devices are not accessed by just anyone when connected to the network. Lastly, Increase transparency by providing consumers with information on how to choose unexpected data uses. This will help the consumer to manage how they use and share their data. The consumers will be able to turn off certain information collection and usage. Security awareness training should be organized to help the users avoid risky behavior while using IoT devices.

F. F. Ways of resolving IoT issues at the organization

- The organization should register every employee's devices that are to be connected to the network. By doing this, they will be able to have control over those devices. This will also help to easily detect an attack surface and block the vulnerability.
- The organization should design a security policy that will engage all the employees or partners in ensuring that the IoT devices are updated and patches implemented when necessary or as soon as the manufacturer makes them available. The update of IoT devices curbs the possibility of hackers penetrating the organizations' network through the IoT devices.
- The organization should employ all the necessary security mechanism to monitor the devices connected to its organizational network to ensure its security policy is implemented. When the security policy of an organization is weak, the device connected to the network becomes a threat surface for attack. The users should be able to implement every security policy the organization has designed to avoid the risk of leaking out sensitive data of both the user and the organization

G. Ways of Safeguarding Data From Unauthorized People in an Organization

According to the [13]Prime Factors Data Protection (2019) Encrypt RIGHT simplifies application-level data protection by abstracting data protection policies from application programming, while providing a complete separation of duties between information security and application programming. Leveraging a Data Security Governance approach, Encrypt RIGHT defines and enforces how data is protected, who may access specific data, and what format that data will take when access is granted (unrestricted, partially masked, or fully restricted). According to Prime most data is left exposed when in use at the application layer! It outlines six ways of protecting data at the application level.

- Encryption: This is the conversion of data into codes so that the original data will not be exposed. It is implemented to encrypt data at the application level. Encryption is normally applied to hide sensitive data especially in payment systems.
- Masking: Masking is used as a data privacy solution to hide vital information. In ATMs cards for example the Permanent Account Numbers (PAN) have some part usually mask on transmission to avoid unauthorized person having access to them. It enables differential privacy with dynamic data masking and role-based access controls
- Tokenization: The use of tokens helps to exchange sensitive data with non-sensitive data with a relationship to the sensitive data. The validation of the sensitive data can only be done by providing the non-sensitive data. It pseudonymizes and anonymize sensitive data for regulatory and industry standards compliance
- Access control: Data access control ensure that a user or individual that is supposed to have access to a particular data has that access and not more than red of access does not have access. It checks the degree of access to sensitive data either in full, partial, or no access.
- Key Management: According [14] Key management refers to management of cryptographic keys in a cryptosystem, it includes dealing with the generation, exchange, storage, use, crypto-shredding (destruction) and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols.
- Traceability: This is about the audit Logs and reports to know who accessed a data and for what. It triggers alerts for traceability of the user and compliance to the standard.

III. METHODOLOGY

This paper presents a comprehensive literature review of sources relating to data privacy and information security in relation to IoT in an organization. An argument using the review's findings from both literature review, other sources and logical inferences is presented to analyze the data Privacy and Security on IoT Devices in an organization with the challenges and resolutions.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

A. Aim

The aim of this study is to critically analyze the data privacy and security on IoT devices in an organization. This study is an explorative study.

B. Objectives of the study

The main objectives of the research are:
The objectives are

- To analyze the issues of data privacy in an organization
- To x-ray the different data and information breaches that could happen in an organization
- To Proffer solution to the challenges of data privacy and security breaches in an organization

IV. CONCLUSION

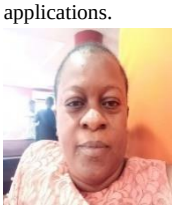
As people get connected every day, it is difficult to stay away from the internet. Even people unknowingly use internet. We have strived to x-rayed the challenges and the different breaches that can occur when using IoT devices in an organization. It is a high risk to have a vulnerable organization due to vulnerable device. Organization can go extinct if they are attacked by an insider or outsider due to vulnerable devices. This is why every organization should conduct awareness trainings for the staff on data privacy and security and ensure that all steps are taken to protect data and information in their organization. The organization should also have a security policy that will guide it employee which in turn will protect the organization in the light of increasing use of IoT in the organization.

REFERENCES

1. NDPR (2019) Nigeria Data Protection Act NDPR.http://www.dataguidance.com
2. S. Von Solms, (2000) “Information security—the third wave?,” Comput.Secur., vol. 19, no. 7, pp. 615–620, 2000. [CrossRef]
3. K. Thomson, R. Von Solms, and L. Louw, “Cultivating an organizational information security culture,” Comput. Fraud Security, no. 10, pp. 7–11, 2006. [CrossRef]
4. National Privacy Commission (2012) https://en.wikipedia.org/wiki/National_Privacy_Commission_(2019)
5. https://www.securitymagazine.com/ (2021) People Risk Management and the Journey to Agile Operational Resiliency retried July 3, 2022
6. Fergus U Onu, Ikechukwu J, Ezea (2022)Critical Analysis Of The Vulnerabilities Surrounding The Use Of POS Services In Rural Nigerian Communities, Published by Blue Eyes Intelligence Engineering and Science, June 2022, ISSN 2394-0913
7. Mohammed Mane (2020) How Ihebuzor Chris, Access Bank Hacker Was Arrested by EFCC https://www.techawkng.com/2020/09/12/how-ihebuzor-chris-access-bank-hacker-was-arrested-by-efcc/ Lagos
8. The Guaridian Newspaper: Man hacks into Nigeria Bank’s System steal N1.87b, Published on August 13, 2021,Lagos Nigeria,
9. MouradeAzrour, Jamal Mabrouki, AzidineGuezzaz, AmbrinaKanwal,(2021)"Internet of Things Security: Challenges and Key Issues", Security and Communication Networks, vol. 2021, ArticleID 5533843, 11 pages, . https://doi.org/10. 1155/2021/5533843 [CrossRef]
10. Aldossary, S. & Allen, W. (2016). Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions. International Journal of Advanced Computer Science and Applications. 7. 10.14569/IJACSA.2016.070464. [CrossRef]
11. Katrenko A and Semeniak E (2021) Internet of Things (IoT) Security: Challenges and Best Practices It was originally publishedonhttps://www.apriorit.com/
12. Atoui R. (2018) The Importance of Security by Design for IoT Devices
13. https://www.primefactors.com/data-protection/ July 2022
14. Dawn M. Turner (2016: What is Key Management? a CISO Perspective https://www.cryptomathic.com Feb, 21, 2016, retrieved July 3 , 2022

AUTHORS PROFILE

Ikechukwu Jonathan Ezea is currently the Country Head Technology & Services, FBNBank Sierra Leone, a subsidiary of First Bank Nigeria Ltd. Prior to his secondment to the subsidiary, he was the Head of ATM/POS Channel Support, First Bank of Nigeria Ltd. He holds MSc. in Information Technology. He is a member Nigeria Computer Society and a Fellow Institute of Information Managers Africa (IIMA). He is presently a Post graduate student at Ebonyi state University Abakaliki. His research interest is in data communication, network and security of banking applications.



Ezeanya Christiana Uchenna is currently working with National Open University of Nigeria as a Network AdministratorShe holds MSc. in Information Technology. She is a member of Nigeria Computer Society and Computer Professionals of Nigeria. Her research area is on data security and privacy.