Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

https://doi.org/10.62643/ijerst.2024.v17.i3.pp16-26

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 3, 2024

DATA PRIVACY IN IOT ECOSYSTEMS

[1]Samatha Nekkalapudi [2]Botla Nandana[3]Attaluri Lalitha [4]Gudapati Sarala

[1, 2, 3,]Asst Professor, Vidya Jyothi Institute Of Technology, Hyderabad

[4]Asst Professor, Sir C R Reddy College For Women, Eluru.

Abstract:

This report presents the results of an exhaustive investigation of data security and privacy concerns. In order to help both businesses and society, the article looked at possible privacy breaches in the IoT ecosystem and how to fix them. Different Internet of Things (IoT) techniques bring up different operational, ethical, security, and privacy problems; this article also looked at the possible reputational damage that these approaches might do to people and society at large. Data analytics, applications, ethical considerations, privacy issues, and operational details of the Internet of Things were all included of the evaluation. Also included in this study is an overview of blockchain technology and its potential applications to the common problems with privacy and security in distributed systems. Topics: Smart healthcare, Blockchain technology, Internet of Things (IoT), data security and privacy.

Key Words: Internet of Things, Data privacy and security, Data analytics, Blockchain technology

I. Introduction:

A network of physical items, or "Things," that can share data with other networks and devices via the Internet is called the Internet of Things (IoT). Every facet of people's, businesses', and society's everyday lives is touched by the Internet of Things (IoT) in some way. Among the many potential uses for the Internet of Things, some of the most prominent are medical and healthcare, irrigation and agriculture, transportation, smart homes, manufacturing (including Industrial IoT), and the automobile industry. Some of the problems with conventional Internet of Things (IoT) apps can be solved with the help of blockchain technology. These problems include safeguarding sensitive data during transmission over the IoT network, reducing the need for a third party to verify IoT data, making the most of the processing power of IoT devices, reducing the operational costs of IoT applications, and many more. Actually, blockchain provides an environment for IoT devices, apps, and platforms that is both decentralized and scalable. In addition, companies may run smart apps and complete a plethora of legal activities between business partners using blockchain-based IoT solutions. There is potential for the creation of an intelligent, secure, decentralized, and scalable Internet of Things (IoT) ecosystem to emerge from the coming together of blockchain

https://doi.org/10.62643/ijerst.2024.v17.i3.pp16-26 ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 3, 2024

technology, AI for IoT applications, cloud computing, and fog computing. However, issues with centralization, data security [2], and scalability are prevalent in IoT systems. Although the idea of an interconnected network of physical devices has been around for some time, the most important technological breakthrough of the 21st century has been the Internet of Things (IoT) due to advancements in several enabling technologies, such as inexpensive and power-efficient sensors, advanced and edge computing, data analytics, machine learning, and the like. Blockchain technology refers to a distributed ledger system that stores immutable records of transactions recorded at certain times and is overseen by a group of computers rather than a single entity [4]. Securely kept as interconnected blocks, these data records are encrypted. Blockchains are distributed ledgers that include immutable data in the form of blocks that are time stamped. They are disseminated over peer-to-peer networks. Cryptographic hash techniques secure and connect all of the transactions in a block. One new development in this open networked system is blockchain technology, which aims to make computing secure, transparent, and decentralized (i.e., not owned by any one company) for all users. A great deal of promise exists for Internet of Things (IoT) cloud infrastructure in the smart healthcare sector. Thanks to devices that are connected to the internet, patient monitoring may now be done remotely and in real-time. Fitness bands, glucometer monitoring cuffs, blood pressure, heart rate monitors, and many more Internet of Things (IoT) wearable gadgets have made personalized health care a reality. Thanks to Internet of Things (IoT) sensors and tagging devices, hospital managers can keep tabs on a range of assets, such as nebulizers, oxygen pumps, wheelchairs, and other monitoring equipment, in real-time. The vast amount of medical data collected from real-world instances utilizing these different IoT devices has greatly improved the accuracy and precision of many services, such as medical treatment, emergency care, resource utilization, insurance claims, resources, medical information systems, etc. Because data is integral to the Internet of Things (IoT) cloud infrastructure, it is especially vulnerable to cyber attacks. The biomedical sector is one of the primary users of blockchain technology, which ensures data integrity by facilitating distributed access control, data lineage, and non-repudiation. Information gathered comes from a variety of sources, including clinical studies, individual biosensors, health insurance, and patient records. Data security and privacy issues are prevalent in distributed systems, and blockchain technology is mostly used to fix them. Additional goals include creating a reliable and transparent healthcare ecosystem and guaranteeing the non-repudiation of medical activities or transactions. By applying blockchain

https://doi.org/10.62643/ijerst.2024.v17.i3.pp16-26 ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 3, 2024

technology to the biomedical domain, the reliability, data privacy, and secure information issues plaguing the IoT paradigm may be remedied. Thanks to data mining tools, we can quickly glean insights from massive data sets that were previously inaccessible. Various public and commercial organizations may now readily gather, store, and handle massive amounts of data, including personally identifiable information, thanks to advancements in computer technology. Data miners may have access to these datasets for use in academic studies. Nevertheless, due to the potentially sensitive nature of the information held in the databases, its publication or outsourcing for study might compromise individuals' privacy. Individuals' privacy is at danger from a variety of disclosure hazards [1]. The challenge, therefore, is to glean useful insights from massive datasets without jeopardizing the security of confidential information that can give rise to a host of moral and societal concerns should it fall into the wrong hands. Consequently, data should be encrypted using appropriate methods prior to data mining [2].

II Literature survey:

1. Leveraging Digital Tools and Technologies to Alleviate COVID-19 Pandemic:

The potential global hazard posed by the new corona virus (COVID-19) illness requires special attention. The identification, control, tracking, and management of diseases; the prediction of outbreaks; the safe exchange of knowledge; data analysis and decision-making processes; and all of this is made possible by a wide variety of digital technologies, including AI-driven applications built upon machine learning (ML), blockchain technology, big data analytics, cloud computing, and the Internet of things (IoT). Healthcare systems, clinical procedures, and therapies are all benefiting from new models made possible by cutting-edge and developing technology. This paper's principal goal is to survey the available digital tools and technology and to identify their possible applications in meeting healthcare needs amid this worldwide health crisis. The following terms are associated with this article: COVID-19, AI, ML, eHealth, blockchain, IoT, biosensors.

2. An Efficient Micro aggregation Method for Protecting Mixed Data:

Microdata protection is made easier using MDAV2k, a multivariate data-oriented micro aggregation approach. The method's inability to safeguard real-world data with mixed values stems

https://doi.org/10.62643/ijerst.2024.v17.i3.pp16-26 ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 3, 2024

from its reliance on numeric data alone. Microdata represented as continuous and categorical attribute values may be better protected using the data-oriented micro aggregation approach that we provide in this research. In order to micro aggregate mixed data and obtain greater k-anonymity with less information loss and a better trade-off between information loss and data disclosure risk, the experimental findings demonstrate that the MDAV2k approach, which has enhanced mixed distance measurement, is the way to go.

3. MDAV2K: A VARIABLE-SIZE MICROAGGREGATION TECHNIQUE FOR PRIVACY PRESERVATION:

Both public and commercial entities are amassing massive databases containing personally identifiable information (PII) pertaining to people's daily lives. In order to uncover valuable insights, data mining methods may be used on these datasets. Data breaches may occur if databases are made public for data mining purposes. So, before making the databases available for data mining, privacy preservation procedures should be used to keep them safe. The statistical disclosure control and data mining communities both employ micro aggregation as a privacy preservation strategy to safeguard micro data. Many academics have researched the Maximum distance to Average Vector (MDAV), a prominent multivariate fixed-size micro aggregation approach. Preserving privacy with little data loss is the main objective of these strategies. A low-information-loss, variable-size-improved MDAV method is proposed in this study.

4. Anonymizing Classification Data for Privacy Preservation:

One of the most basic challenges in data analysis is classification. A massive dataset must be accessible in order to train a classifier. There is a risk to individuals' privacy when personally identifiable information (PII) like customer records or medical histories is made public. It is still feasible to trace the identities of leaked data using a mix of non-identifying variables like {Sex, Zip, Birth date}, even if explicit identifying information like Name and SSN has been removed. A practical method for preventing linking attacks, known as k-anonymization [1], involves masking the linking characteristics so that for every possible combination of linking attribute values, at least k released records meet the criteria. Optimal k-anonymization that minimizes a data distortion

https://doi.org/10.62643/ijerst.2024.v17.i3.pp16-26 ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 3, 2024

metric has been the subject of previous studies. Our main point is that the classification objective—which is to determine the structure of prediction on the "future" data—has nothing to do with reducing distortion in the training data. We provide a k-anonymization method for categorization in this work. Our objective is to discover a k-anonymization that maintains the classification structure, albeit it may not be ideal in terms of avoiding data distortion. To determine how anonymization affects categorization on future data, we ran extensive trials. Experiments using real-world data demonstrate that even with stringent anonymity restrictions, classification quality may be maintained.

5. Machine Learning Based Sentiment Analysis for Text Messages:

Social networking and the dissemination of personal views and ideas are two main functions of popular internet sites like Face book, Twitter, etc. The postings on these sites are what really do the sharing. The use of machine learning algorithms for sentiment analysis or opinion mining on these postings is very significant. In most cases, polarity calculations, subjectivity analysis, or sentiment analysis are used to do the analysis. Using supervised machine learning methods, we analyzed the sentiment of text messages in this research. Online product reviews, casual tweets on Tweeter, and reviews of movies make up the bulk of them. Prior to sentiment analysis, messages undergo pre-processing using three distinct machine learning methods: Naïve Bayes, Decision Tree, and Support Vector Machine (SVM). Topics - Twitter, Sentiment Analysis, Machine Learning, Natural Language Processing

6. Porous Silicon-Based Biosensors: Towards Real-Time Optical Detection of Target Bacteria in the Food Industry:

Ensuring a secure food supply and preventing food borne infections depend on the rapid identification of target germs. Our optical biosensor can detect and quantify Escherichia coli (E. coli) in complicated process water from the food sector, a typical indicator bacterium. A thin sheet of nanostructure, oxidized porous silicon (PSi) imbued with E. coli-specific antibodies forms the basis of the biosensor. In order to measure the biosensors' reflectivity spectra in real time, water samples were taken immediately from the processing lines of freshly cut produce. Complex natural microflora (microbial load > 107 cell/mL), soil particles, and plant cell debris were all present in the process water. It has been shown that the biosensor's thin-film optical interference spectra

International Journal of Engineering Research and Science & Technology

https://doi.org/10.62643/ijerst.2024.v17.i3.pp16-26

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 3, 2024

undergo strong and predictable alterations when culture-grown E. coli is introduced into the process water. The second is due to the fact that the target cells are captured onto the biosensor surface in a very precise manner, as verified by the real-time polymerase chain reaction (PCR). Even though the quantity of target cells was orders of magnitude lower than other bacterial species, the biosensors were able to selectively detect and quantify them without the need for pre-enrichment or processing.

7. The Internet of Things (IoT): An Overview:

Every action we do is dictated by ICT, or information and communications technology. Integrating diverse gadgets into a single network, it is becoming an essential component of our daily lives. To mention only a few examples, there is personal computing, sensing, surveillance, smart homes, entertainment, transportation, and video streaming. New technology, apps, protocols, and algorithms are constantly appearing on the Internet as a result of its ongoing evolution and change. Internet connection and mobile broadband are experiencing a period of rapid innovation due to the acceleration of wireless communication trends. More and more, infrastructure-free communication devices are becoming smaller, smarter, more powerful, more connected, less expensive, and simpler to install and deploy. The introduction of the Internet of Things (IoT) signals a fresh course for the information and communication technology (ICT) industry's future. Once known as Machine-to-Machine (M2M) communications, the Internet of Things (IoT) is now a major focus in the information and communication technology (ICT) industry and academic circles. The Internet of Things (IoT) paradigm, including its ideas, principles, and prospective advantages, are reviewed in this work. Our primary emphasis is on the core technologies, new protocols, and extensive uses of the Internet of Things (IoT). Anyone venturing into the Internet of Things (IoT) realm with the intention of comprehending and contributing to its evolution may find this overview useful. Smart objects, heterogeneous devices, ICT, IOT, and machine-to-machine communication are all part of this larger framework.

https://doi.org/10.62643/ijerst.2024.v17.i3.pp16-26 ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 3, 2024

8. Efficient Location Privacy Algorithm for Internet of Things (IoT) Services and Applications:

The fast growth of IoT technology, together with the pervasiveness of smart phones and social media, has made location-based services (LBS) a crucial field of study. While the LBS with IoT offers a lot of benefits, like ease and flexibility, consumers run the risk of having their privacy compromised. Unreliable or malevolent LBS servers that have access to all user data have the ability to follow users in different ways or disclose personal information to other parties. To begin, we take a look at the state of the art in location privacy preservation algorithms—the dummy-location selection (DLS) method—and then we create an attack algorithm for DLS (ADLS) to put new Internet of Things (IoT) security measures to the test. We provide a new dummy location privacy-preserving (DLP) method that takes into account computational costs and different users' privacy needs in order to effectively preserve user's location privacy. The suggested schemes' efficacy has been assessed using comprehensive simulation tests. From the evaluation findings, it is clear that the ADLS algorithm outperforms the DLS algorithm in determining the user's actual position relative to the selected dummy locations. While maintaining the same degree of privacy as the DLS method, our suggested DLP algorithm offers many benefits over it, including a reduced likelihood of exposing the user's actual location and enhanced computational efficiency in terms of time, speed, accuracy, and complexity. The following terms are essential: k-anonymization, privacy preservation, location privacy, location-based services.

9. Towards Collaborative Intelligent IoT eHealth: from Device to Fog, and Cloud:

Recent years have seen a sea change in the way technology and healthcare interact, thanks to developments like the intelligent Internet of Things (IoT), artificial intelligence (AI), and the widespread use of medical-grade wearables. Personalized services, customized information, enhanced availability and accessibility, and cost-effective distribution were some of the ways in which the healthcare sector benefited from the AI-powered IoT's revolutionary advances and unique potential. There are still a lot of obstacles to overcome in the healthcare system's shift from being focused on clinics to patients, despite these promising developments. Improving critical metrics like latency, availability, and real-time analytics via the use of hierarchical and collaborative architectures is essential for unlocking and enabling this horizon shift. Using the idea

https://doi.org/10.62643/ijerst.2024.v17.i3.pp16-26 ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 3, 2024

of a Collaborative Machine Learning method, we provide an all-encompassing AI-driven Internet of Things (IoT) eHealth architecture in this study. This architecture distributes intelligence across three layers: Device, Edge/Fog, and Cloud. This system enhances the decision-making ability by allowing healthcare practitioners to continually monitor patients' health-related data anywhere, at any time. They can then deliver real-time actionable insights. An extensive case study based on electrocardiogram (ECG) arrhythmia detection is used to examine the practicability of such an architecture. From the mapping and deployment of advanced machine learning techniques (e.g., Convolutional Neural Network) to the proposed architecture, this illustrative example covers and addresses all important aspects, including design implications such as corresponding overheads, energy consumption, latency, and performance.

III. Existing system:(Problem Statement)

Problems with data security and privacy were investigated thoroughly. In order to help both businesses and society, the article looked at possible privacy breaches in the IoT ecosystem and how to fix them. Different Internet of Things (IoT) techniques bring up different operational, ethical, security, and privacy problems; this article also looked at the possible reputational damage that these approaches might do to people and society at large.

IV. Proposed system:

From simple electronics to complex mobile and industrial machinery, all of these items are part of the Internet of Things (IoT), which allows them to communicate with each other directly, without the need for a human intermediary. Security and privacy remain major worries in light of the Internet of Things' (IoT) many societal and technical advantages and enormous commercial possibilities. Recent studies and discussions on blockchain technology's use in the biomedical field are examined in this article. It provides practical answers to problems with privacy and security in the Internet of Things (IoT). It takes a look at the many kinds of assaults on the Internet of Things (IoT), with an emphasis on DDoS attacks and possible ways to protect against them. While the idea of using blockchain technology to mitigate distributed denial of service (DDoS) assaults on

International Journal of Engineering Research and Science & Technology

https://doi.org/10.62643/ijerst.2024.v17.i3.pp16-26

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 3, 2024

the Internet of Things (IoT) is still in its early stages, this article provides some suggestions on where the field may go from here.

Methodology:

Security challenges of IOT:

- **Rogue IoT Devices Detection:**

The recommended method of connecting Internet of Things (IoT) devices is Wi-Fi. On the other hand, rogue access points (APs) or devices with identical SSIDs and/or MAC/IP addresses to authorised devices can spoof Wi-Fi connections and conduct attacks. It's possible that traditional network security mechanisms can't prevent such attacks. For the purpose of gathering or manipulating private data, a rogue device impersonates or joins the original device's group [12]. It asserts that it is acceptable to exchange and acquire data produced by other IoT devices for nefarious purposes. The network's perimeter may be violated by rogue IoT devices. Without the owners' knowledge, devices like the Raspberry Pi can be turned into a malicious AP (Access Point) that intercepts incoming data transfers.

Using IoT bots to mine cryptocurrency:

Over the past decade, cryptocurrencies have witnessed great growth in popularity, and the risk associated with IoT security has also increased significantly. Cryptocurrencies can be purchased through a number of unusual techniques.

Cryptocurrency mining is known to require significant CPU and GPU resources, which leads to the

https://doi.org/10.62643/ijerst.2024.v17.i3.pp16-26 ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 3, 2024

use of IoT bots and another security risk for the IoT [13]. These Internet of Things (IoT) bots or botnets assault IoT devices without causing any damage to them while covertly mining cryptocurrency. One such illustration is the open-source cryptocurrency Monero, which was the first to be mined via IoT botnets. A device like a video camera might not be ideal for bitcoin mining due to its resource limitations, but a group of video cameras might be able to. Because a single attack by such botnets might flood and disrupt the entire market, IoT botnet miners constitute a serious threat to the cryptocurrency industry.

Conclusion:

IoT includes a variety of devices, from basic electronics to mobile and industrial equipment, where communication occurs directly between devices without the involvement of a human. Despite the IoT's many technological and social benefits and immense economic potential, security and privacy are still important concerns. The article examines recent findings and discuses about blockchain technology's uses in the biomedical industry. It mostly focuses on IoT security and privacy issues and offers some viable solutions. It examines the various IoT attacks with a focus on distributed denial of service attacks and potential countermeasures to lessen such attacks. The article offers potential research topics for future studies in leveraging the blockchain to reduce DDoS attacks in IoT, which is an active research area and in its infancy.

References:

[1] Chettri S, Debnath D, Devi P. Leveraging digital tools and technologies to alleviate COVID-19 pandemic. Available at SSRN 3626092. 2020 Jun 11.

[2] Nongbri I, Hadem P, Chettri S. A survey on single sign-on. Int. J. Creative Res. Thoughts. 2018 Apr;6(2):595-602.

[3] Chettri SK, Borah B. An efficient micro aggregation method for protecting mixed data. In Computer Networks & Communications (NetCom) 2013 (pp. 551-561). Springer, New York, NY..

[4] Chettri SK, Borah B. MDAV2K: a variable-size micro aggregation technique for privacy preservation. In International conference on information technology convergence and services, In 2012 Jan 4 (pp. 105-118)..

[5] Borah B. Anonymizing classification data for preserving privacy. In International Symposium on Security in Computing and Communication 2015 Aug 10 (pp. 99-109). Springer, Cham..

https://doi.org/10.62643/ijerst.2024.v17.i3.pp16-26 ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 3, 2024

[6] Bhagat A, Sharma A, Chettri S. Machine learning based sentiment analysis for text messages. International Journal of Computing and Technology. 2020 Jun 20.

[7] Chettri SK, Paul B, Dutta AK. Statistical Disclosure Control for Data Privacy Preservation. International Journal of Computer Applications. 2013 Jan 1;80(10).

[8] Paul B, Chettri SK. Smart City: Recent Advances and Research Issues. Inventive Systems and Control. 2021:77-92.

[9] Saikia M, Chakraborty S, Barman S, Chettri SK. Aptitude Question Paper Generator and Answer Verification System. In Recent Developments in Machine Learning and Data Analytics 2019 (pp. 129-136). Springer, Singapore.

[10] Chettri SK, Paul B, Dutta AK. A comparative study on micro aggregation techniques for Micro data protection. International Journal of Data Mining & Knowledge Management Process. 2012 Nov 1;2(6):27..

[11] Chettri SK, Borah B. Privacy Preservation of Time Series Data Using Discrete Wavelet Transforms. In Advanced Computing, Networking and Informatics-Volume 2 2014 (pp. 249-258). Springer, Cham.

[12] Debnath D., Chettri S.K., Dutta A.K. (2022) Security and Privacy Issues in Internet of Things. In: Fong S., Dey N., Joshi A. (eds) ICT Analysis and Applications. Lecture Notes in Networks and Systems, vol 314. Springer, Singapore. https://doi.org/10.1007/978-981-16-5655-2_7

[13] Debnath D, Chettri SK. Blockchain: Application Domains, Research Issues and Challenges. Computer Networks, Big Data and IoT. 2021:115-29..

[14] Debnath D, Chettri SK. Internet of Things: Current Research, Challenges, Trends and Applications. In Applications of Artificial Intelligence in Engineering 2021 (pp. 679-694). Springer, Singapore.

[15] Chettri SK, Ray BK. On Analysis of Mixed Data Classification with Privacy Preservation. ADBU Journal of Engineering Technology. 2016 Mar 1;4.