Commentary
Volume 11:3, 2022

International Journal of
Sensor Networks and Data Communications

ISSN: 2090-4886 Open Access

Data Security and Privacy

Brent Harris*

Department of Computing, Imperial College London, London, UK

Description

Organizations must take precautions to safeguard the privacy and security of the personal data they collect. However, how can consumers tell if an organization made reasonable precautions to secure their data when it is breached? When penetrated organizations tell impacted individuals, this communication is likely to be one of the few outside windows into the occurrence, and it can become a valuable study artefact. The goal of this desktop study was to see how well publicly accessible Australian data breach notifications reflected data privacy and security best practices [1]. The results of a qualitative content analysis of 33 publicly available Australian data breach messages are presented in this study, together with a brief assessment of literature and government guidelines on data security and privacy best practices. This investigation revealed that data privacy and security procedures were not adequately reflected. The content analysis, literature, and government guidelines were utilized to inform and design a new voluntary framework for organizations. This is made up of a set of questions separated into two categories: responsible data management and appropriate breach presentation.

The framework has the potential to assist businesses in incorporating data privacy and security management features into their data breach communications. This might help businesses meet their legal and ethical obligations to account for their activities in maintaining the privacy and security of the personal data they collect. In the current context, traditional healthcare systems use centralized client-server architecture to store and handle patient-health data. Due to technical and architectural restrictions, data housed in each healthcare institution is kept in silos and cannot be easily shared with other institutions. In the instance of a person visiting many hospitals, hospitals lack an effective and secure data exchange method, resulting in monetary and resource loss.

Block chain, a disruptive technology with a safe and dependable decentralized foundation, may be utilized to solve difficulties in traditional healthcare architecture by storing, sharing, and retrieving electronic health records securely (EHR) [2]. This study proposes a block chain-based architecture for EHR in healthcare administration that is connected with the Interplanetary File System (IPFS). This suggested system would allow healthcare organizations to maintain decentralized, fail-safe, and tamper-proof healthcare ledgers. Hospitals and physicians are lightweight nodes, whereas patient nodes can be either full or light. For combating false node attacks, the model provides two-factor authentication and multi-factor authentication [3].

Patients may serve as digital stewards for personal health data by granting on-demand access to physicians and hospitals and removing it once a set amount of time has passed. Health combines data from, lifestyle, environment, social media, medical records, and medical insurance claims to provide tailored care, prevent and anticipate sickness, and precise therapies [4]. It makes substantial use of sensing (e.g., electronic health monitoring devices), computing (e.g., machine learning), and communication technologies (e.g., interaction between the health data name of the patient and the career, as well as the patient's medical problems, it must be handled with caution at all times. Leakage centers). Because health data contains sensitive personal information such as the of this sensitive information has ramifications in one's personal life, such as bullying, increased insurance premiums, and job loss owing to medical history [5].

References

1. Ouadine, Ahmed Youssef, Mostafa Mjahed, Hassan Ayad, and Abdeljalil El Kari. "UAV quadrotor fault detection and isolation using artificial neural network and hammerstein-wiener model." *Stud Inform Control* 29 (2020):317-328.
2. Fu, Lili, and Yinhong Dong. "Research on internet search data in China's social problems under the background of big data." *J logist Inform Serv Sci* 5 (2018): 55-67.
3. Banciu, Doina, Mirelille Radoi, and Stefan Belloiu. "Information security awareness in Romanian public administration: An exploratory case study." *Stud Inform Control* 29 (2020): 121-129.
4. Naoui M.A., L. Brahim, M. Ayad. "Integrating iot devices and deep learning for renewable energy in big data system." *UPB Sci Bulletin Series C: Electrical Times* 82 (2020): 251-266.
5. Song, Mingoo. "Development of big data system for energy big data. KIISE transactions on computing practices." 24 (2018): 24-32.

How to cite this article: Harris, Brent. "Data Security and Privacy." J Sens Netw Data Commun 11 (2022): 150.

***Address for Correspondence:** Brent Harris, Department of Computing, Imperial College London, UK; E-mail: BrentHarris@gmail.com*

Received: 02 March, 2022, Manuscript No. sndc-22-65178; **Editor Assigned:** 04 March, 2022, PreQC No. P-65178; **Reviewed:** 16 March, 2022, QC No. Q-65178; **Revised:** 21 March, 2022, Manuscript No. R-65178; **Published:** 28 March, 2022. DOI: 10.37421/2090-4886.2022.11.150