RESEARCH ARTICLE

SAMRIDDHI Volume 14, Special Issue 2, 2022 Print ISSN : 2229-7111 Online ISSN : 2454-5767

Study of Data Privacy and User Data Control

Abhijit Banubakode[1*], Solomon Darshi[2], Daulappa Bhalke[3]

[1*,2] MET Institute of Computer Science, Mumbai, India; e-mail*: abhijitsiu@gmail.com

[3] AISSMS College of Engineering Pune, India.

ABSTRACT

Data is information in the form of facts or statistics obtained from a variety of sources that must be analysed, processed, and used to aid decision-making, or information in an electronic form that can be stored and accessed by a computer. In a world with ever-growing amounts of data, privacy is a crucial topic to scrutinize. Privacy of data defines the practices which checks the data shared by users is only used for its valid purpose. It focuses on the proper handling of sensitive data, such as personal data but also other private data, such as some important data and intellectual property data, in order to meet the criteria while simultaneously protecting the data's secrecy and invariability. Data control is the management of information strategies for a company's data. Data control, unlike data quality, focuses on observing and reporting on how processes are performing as well as controlling faults. Inspection, validation, alerting, documentation, issue reporting, and issue tracking are all functions. In this paper we have conducted survey of software users who are using spy-ware or antitheft software's to prevent breaches.

Keywords- Confidential, Privacy, Electronic, Intellectual

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, (2022); DOI : 10.18090/samriddhi.v14spli02.8

INTRODUCTION

Privacy, in simple words, is the individual's right, organizations or groups to check who can see, access, or manipulating some property, such as their bodies, ideas, data, or information. Control is obtained by an individual through physical, public, or descriptive boundaries that help prevent unwanted access, observation, or use.

Let's consider some example,

- A locked front door can act as a physical boundary that helps prevents strangers from entering a house without direct permission in the form of a key to open the door or a person inside opening the door.
- A members-only club demonstrates public boundary which only allows members to access and use club resources.
- A non-disclosure agreement defines descriptive boundary and restricts what data can be shared with others[1].

Data privacy has become more important as the number of individuals utilising the Internet has increased. Websites, software, and social media platforms commonly need to gather and keep personal data in order to provide services users.

On the other side, some programmes and platforms may go beyond users' expectations in terms of data collection and use, leaving them with less privacy than they intended. Other apps and platforms may not have sufficient controls in place to protect the data they gather, potentially resulting in a data breach that compromises user privacy. Other apps and platforms may not put enough controls in place to protect the data they collect, which could lead to a data breach that threatens user privacy.

Corresponding Author : Abhijit Banubakode, MET Institute of Computer Science, Mumbai, India; e-mail : abhijitsiu@gmail.com

How to cite this article : Banubakode, A., Darshi, S., Bhalke, D. (2022). Study of Data Privacy and User Data Control.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, Volume 14, Special Issue (2), 244-248.

Source of support : Nil

Conflict of interest : None

Because of the rapid rise of the global information economy, which is fuelled by new technologies and innovative business models, an ever-increasing quantity of user data is gathered, processed, traded, examined, preserved, and occasionally exploited for commercial reasons. This also implies that the amount of data leaks, whether unintentional or purposeful, inaccurate or deleted data records, and data abuse instances is on the rise[4]. As more than just a consequence, the need for data privacy has increased, as has the demand for data security. Data privacy refers to the right to regulate how personal information is gathered, exchanged, and utilized, preserved, or erased. It's difficult, but not unachievable, to find a balance between an individual's right to data privacy and an organization's wish to use personal data for its own reasons[5][6].

HISTORY

According to Yahoo, a group of hackers penetrated the firm in August 2013, compromising 1 billion accounts. In this situation, security questions and answers were also hacked, enhancing the risk of identity theft. While in talks to sell itself to Verizon, Yahoo first reported the vulnerability on December 14, 2016. Yahoo required all affected users to change their passwords and re-encrypt any security questions and answers that were not encrypted.

Impact: 3 billion accounts

In March 2018, it was reported that the personal information of over a billion Indians stored in the world's largest biometric database might be digitalized.

This massive data breach was caused by a data leak on a system maintained by a state-owned electricity company. The breach exposed the sensitive information of Aadhaar cardholders, including their names, 12-digit identity numbers, photos, thumbprints, retina scans, and other identifying traits, as well as the bank details of nearly every Indian citizen.

Impact: 1.1 billion people

In May 2018, Twitter users were notified of a problem that exposed passwords in internal logs, making all user credentials public to the local network. Despite the fact that the weakness had been fixed and there was no indication of a breach or abuse, Twitter encouraged its 330 million internet users to update their passwords as a precaution, the company indicated that the password update was recommended as a precaution. Twitter did not specify how many users were affected, only that there were a large number of them and that they had been exposed for a long period.

Impact: 330 million users

eBay was the victim of an encrypted password leak in February and March 2014, prompting the company to ask all of its 145 million customers to reset their passwords. To get access to this wealth of user data, the attackers exploited a tiny collection of staff credentials. Data stolen included encrypted passwords and other personal information such as names, e-mail addresses, physical addresses, phone numbers, and dates of birth. The vulnerability was discovered in May 2014 after a one-month examination by eBay.Impact: 145 million users.

In April of 2020, when Zoom signups were hitting their epidemic peak, hackers hacked 500,000 accounts and sold or freely released them on the dark web. Hackers first explored the dark web for previously stolen login information going all the way back to 2013. Because passwords are often reused, they had immediate access to a large number of current Zoom accounts. To exploit the remaining accounts, a number of credential stuffing assaults were initiated. Those who received hacked Zoom accounts were allowed to join live streaming meetings.

Impact: 500,000 users.

RISKS

Accidental Exposure

A substantial number of data breaches are the consequence of careless or inadvertent disclosure of sensitive data, rather than a deliberate attack. Employees of a company frequently disclose, allow access to, lose, or mishandle sensitive information, either by mistake or because they are unaware of security standards.

An employee downloading a spreadsheet with confidential data to a cloud service and neglecting to password secure it might result in accidental disclosure.

Phishing and Other Social Engineering Attacks

Social engineering is a common tactic used by attackers to get access to sensitive data. Persuading or misleading someone into giving personal information or granting access to private accounts are examples of these crimes.

Phishing is a sort of social engineering that has

become increasingly prevalent. Messages that appear to come from a trustworthy source but are really sent by an attacker are involved. If a victim agrees, such as by submitting private information or clicking on a malicious link, attackers can corrupt their device or get access to a company's network.

Insider Threats

Employees that mistakenly or actively compromise the privacy of an organization's data are known as insider threats. Insider risks can be divided into three categories:

- Un-Intentional Insider – These are users who may inflict harm through accident, ignorance, or a lack of understanding of security measures.
- Intentional Insider - These are users that are deliberately attempting to steal data or harm the company for personal benefit.
- Compromised Insider - These are people who are unaware that an external attacker has gained access to their accounts or credentials. The intruder can then engage in harmful behaviour while posing as a genuine user[15].

Ransomware

Ransomware is a serious threat to data in companies of all sizes. Ransomware infects computers and encrypts data, making it useless until the decryption key is delivered. Attackers display a blackmail notice seeking money in exchange for the key; however, paying the ransom is often ineffective, and the data is destroyed[6][7].

Many types of ransomware have the capacity to quickly propagate and infect large parts of a company's network. If a company does not keep frequent backups or if the ransomware affects the backup systems, there is absolutely no way to recover.

Data Loss in the Cloud

To make sharing and collaboration easier, many firms are transferring their data to the cloud. However, moving data to the cloud makes it more difficult to maintain and avoid data loss. Data is accessed using personal devices and unprotected networks. It's all too easy to share a file with unauthorised people, either accidentally or on purpose.

Data loss can lead to a variety of problems, including damage to your image and reputation, as well as lawsuits from customers whose sensitive information has been disclosed and/or destroyed.

SQL Injection

SQL Injection (SQLi) is a popular method for attackers to obtain unauthorised access to a database, steal data, and execute undesired activities. It operates by injecting malicious code onto what seems to be a harmless database query. SQL injection modifies SQL code by inserting special characters into user input that alter the query's context. Instead of processing user input, the database begins executing malicious code that furthers the attacker's objectives. SQL injection can disclose consumer information, intellectual property, or allow attackers administrator access to a database, all of which can have serious implications [10][12].

Insecure coding approaches are the most common cause of SQL injection problems. SQL injection is reasonably straightforward to avoid if programmers adopt safe means for taking input from user, which are readily accessible.

RESEARCH

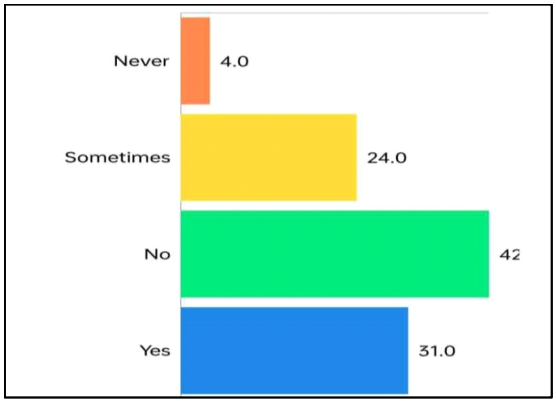

Figure 1: Statistics of people using spy-ware or antitheft software to prevent breaches

Figure 1 shows the statistics of people using spy-ware or antitheft Software to prevent breaches the results revealed that people who are not using antitheft softwares are more as compare people who are using antitheft software. Number of people using antitheft software are 31 and number of people not using antitheft software are 42. The number of people who use antitheft software sometimes are 24 and the number of people who never use antitheft software are 4. Antitheft software is simple to use and responds quickly, according to all responders. Antitheft software is one of the most popular and is available for free, according to the respondents. It is the most popular among the respondents since it allows for group and

individual talking and video conferencing, as well as publishing images and keeping up with current events. LinkedIn is primarily utilised by those who are still employed or self-employed, hence its user base is smaller than that of other social media networks.

As data is generated, edited, processed, or sent, the categorization can be updated. It would be beneficial if you additionally devised steps to prevent users from inflating the categorization degree. Only authorized users should be able to update or degrade data classifications, for instance.

A data use policy is required

Data classification isn't enough; you'll also need a policy that spells out the different forms of access, classification- based parameters for access to data, who has access to the data, what makes proper data usage, and so on. Limit user access to specific regions and deactivate after they've completed the task.

Remember that any rules violations should result in severe consequences.

Keep an eye on who has access to critical information

You must provide the proper access controls to the appropriate user. Restrict access to information using the least privilege principle, which states that just the privileges required to carry out the original purpose should be granted. This will ensure that the data is only used by the appropriate user. Here are a few essential permissions that you may set:

Full control: The user has complete control over the data. This covers data storage, access, modification, deletion, permissions, and more.

Modify: Data may be accessed, modified, and deleted by the user.

Access: The user has access to the data but cannot change or remove it.

Access and modify: Data may be accessed and modified by the user, but it cannot be deleted.

Protect data on a physical level.

Protect your data with endpoint security technologies

When it comes to data security best practises, physical security is sometimes disregarded. You might begin by blocking your workstations while they are not in use, ensuring that no gadgets are physically taken from the premises. This will protect your hard discs and other critical data storage components.

Setting up a BIOS passcode to prevent thieves from launching into your operating systems is another good data security technique. Storage devices, Bluetooth gadgets, cell phones, tablets, and computers all need to be looked after.

Make a list of your cybersecurity policies

Endpoints on your network are continuously under attack. As a result, it's critical to put up a strong endpoint security services to reduce the risk of data breaches. You can begin by putting the following safeguards in place:

Antivirus software: Antivirus software should be installed on all servers and workstations. Conduct frequent scans to keep your system healthy and to detect any infestations, such as ransomware.

Antispyware: Spyware is a type of harmful computer software that is installed without the user's consent. Its primary goal is to gather information about user activity and personal information. Anti-spyware and anti-adware programmes can assist you in removing or blocking these threats. Put them in place.

Firewalls: Firewalls operate as a wall between your data and fraudsters, which is why most experts advocate them as one of the greatest data protection methods. Internal firewalls can also be installed to give additional security.

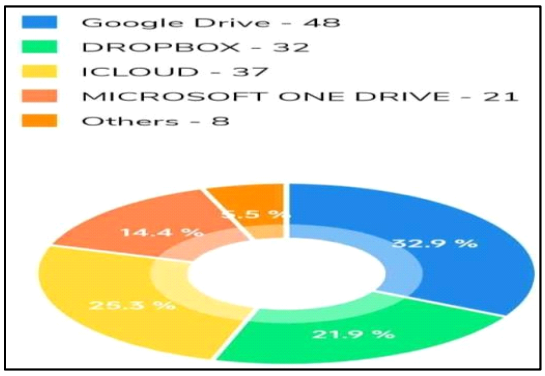

Figure 3: Statistics based on people reference of cloud storage based on afety measures

Table-1: Percentage Of People Using Software's

Sr. No.	Software's	% of Use
1	Google Drive	32.9%
2	Dropbox	21.9%
3	ICloud :	25.3%
4	Microsoft One Drive	14.4%
5	other cloud storages	5.5%

Table-1 describe the ppercentage of people using Google Drive is 32.9%, percentage of people using Dropbox is 21.9%, percentage of people using ICloud is 25.3%, percentage of people using Microsoft One Drive is 14.4% and the percentage of people using other cloud storages is 5.5%.

CONCLUSION

According to the report, the majority of users utilise Google Drive since it is a popular application with excellent collaboration features and strong built-in security. There are, however, techniques to improve the security of information in the cloud. To improve data security, enable two-factor authentication, review security dashboards on a regular basis, discover and classify the data saved in your company's Google Drive, and automate backups. Google Drive is, for the most part, safe from hackers. In addition to native encryption, features such as two-factor authentication and Endpoint Management's security tools can help you avoid security breaches. Data security recommended practises aren't limited to the preventative measures listed above. There's a lot more to this than, including making frequent backups of all data, encrypting data in transit, and enforcing secure password habits, among other things. However, user must recognise that cybersecurity does not include the complete elimination of all threats—this is impossible to do. It's also something user shouldn't overlook. User may at least limit hazards to a significant extent by using the appropriate security measures.

REFERENCES

[1] Flood, C. M. (2011). *Data Data everywhere: Access and* accountability? McGill-Queen's University Press.

[2] Garcia-Alfaro, J. (2012). Data Privacy Management and autonomous spontaneus security: 6th International Workshop, Dpm 2011, and 4th International Workshop, setop 2011, Leuven, Belgium, September 15-16, 2011: Revised selected papers. Springer.

[3] Navarro-Arribas, G., & Torra Vicenc'. (2015). Advanced research in data privacy. Springer.

[4] Rotenberg, M., Scott, J., & Horwitz, J. (2015). Privacy in the modern age: The search for solutions. New Press, The.

[5] 2021. DATA PROTECTION AND PRIVACY. [S.I.]: HART PUBLISHING.

[6] Salomon, David. Data Privacy. Springer, 2003.

[7] Venkataramanan, Nataraj, and Ashwin Shriram. Data Privacy. Chapman & Hall/CRC, 2016.

[8] Lenhard, Thomas H. *Data Security*. Springer, 2022.

[9] Abi Tyas Tunggal. *The 63 Biggest Data Breaches (Updated for February 2022) | UpGuard*. www.upguard.com, 24 Feb. 2022.

[10] GRUENBERG, CAITLIN. *6 Security Controls You Need For General Data Protection Regulation (GDPR) | CyberGRX*. www.cybergrx.com.

[11] Gentry, C., Halevi, S., Smart, N.P9(2012).: Homomorphic evaluation of the AES circuit. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 850–867. Springer, Heidelberg

[12] Hsu, C.Y., et al.(2012): Image feature extraction in encrypted domain with privacy-preserving SIFT. IEEE Trans. Image Process. **21**(11), 4593–4607 (2012)

[13] Lu, W., et al.(2009): Enabling search over encrypted multimedia databases. In: IS&T/SPIE Electron. Imaging, ISOP, February 2009. 725418–725418-11

[14] Song, D.X., et al(2000).: Practical techniques for searches on encrypted data. In: Proceedings of IEEE S&P, pp. 44–55. IEEE

[15] Agrawal, R., et al.(2004): Order preserving encryption for numeric data. In: Proceedings SIGMOD, pp. 563–574. ACM .

[16] Paillier, P.(1999): Public-key cryptosystems based on composite degree residuosity classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223–238. Springer, Heidelberg

[17] El Gamal, Taher(2020): A public key cryptosystem and a signature scheme based on discrete logarithms. In: Blakely, G.R., Chaum, David (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 10–18. Springer, Heidelberg