A Data Security System in The Domain of Online Data Storage

Pradeep Kumar Shah, Assistant Professor,
College of Computing Sciences and Information Technology, Teerthanker Mahaveer University,
Moradabad, Uttar Pradesh, India
Email Id- pradeep.rdndj@gmail.com

ABSTRACT: Data security is a collection of protocols and tools that guard against the accidental or purposeful loss, alterations, or disclosure of data. Control activities, physical security, logical controls, organizational standards, and other protecting approaches that restrict access to unauthorized or malicious persons or processes are only a few of the methods and technologies that may be used to apply data security. In the context of big data, this article gives an overview of data security and data quality. By highlighting the potential conflicts that may arise during the installation of data security and data quality control systems, the author hopes to draw attention to them. Conflict of this nature increases complexity and demands unique, customized solutions. The future scope of this study Information and communications technology (ICT) has been used more often recently by state authorities as well as the corporate sector to access personal data. Data is a crucial component of freedom for both private and public goals.

KEYWORDS: Access, Businesses, Data Security, Encryption, Information, Protection, Sensitive, Systems,

1. INTRODUCTION

The technique of preserving digital information over its full life cycle to preserve it against corruption or unauthorized access is known as data security. Everything is covered, including access and administrative controls, organizational policies and procedures, hardware, software, storage, and user devices [1]. Tools and techniques used in data security make it easier to see how a company's data is being utilized. Through techniques like data masking, encryption, and redaction of sensitive information, these technologies can secure data. Additionally, the approach aids businesses in streamlining auditing procedures and adhering to data protection laws that are becoming stricter. A business may defend its data from cyberattacks by using a solid data security management and planning procedure. Additionally, it aids in reducing the danger of insider threats and human mistakes, which continue to be major contributors to data breaches [2].

Data security is crucial for enterprises across all sectors and geographies for a variety of reasons. Legally, businesses must safeguard user and customer information to prevent its loss or theft and eventual misuse. For instance, the General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and are examples of industry and state rules that highlight an organization's legal responsibilities to safeguard data [3]. Additionally essential to avoiding the reputational cost associated with a data breach is data security. Customers may lose faith in a company as a result of a high-profile breach or data leak and choose to do business with a rival. Along with penalties, court costs, and damage restoration, if sensitive data is destroyed, this also carries the possibility of substantial financial losses. By focusing on the advantages, which are described in greater detail below, data security may be more easily defined [4].

- Secures your information: You can prevent sensitive data from getting into the wrong hands by developing a mentality that is concerned with data security and putting in place the appropriate tools. Sensitive data might contain, among other things, identifying information, healthcare records, and client payment information. This information is kept safe and secure using a data security program designed to match the unique demands of your firm [5].
- Keeps your reputation untainted: Customers trust your company with their sensitive information when they transact businesses with you, and a data security plan enables you to give them the security they require. Your prize has a fantastic standing in the eyes of customers, partners, and businesspeople in general [6].
- Increases your competitiveness: Data breaches are widespread in many businesses, so if you can protect data, you can differentiate yourself from the opponent, which could be having trouble doing the same.
- Reduces the cost of support and development: Incorporating data security measures earlier on in the development cycle might save you money later on when it comes to creating and releasing updates or correcting code issues [7].

1.1 Types of data security:

To protect their people, devices, networks, and systems as well as their data, organizations can utilize a variety of data security types. To create the most effective approach possible, firms should integrate some of the most popular kinds of data security, such as [8].

- Encryption:

Data encryption is the process of scrambling data and concealing its real meaning using algorithms. Data encryption makes sure that only receivers with the right decryption key may see communications. This is important, particularly in the case of a data breach, since even if an attacker is successful in gaining access to the data, they will also not be capable of reading it without the descriptor. Solutions like smart contracts, which secure data as it travels across an organization's complete IT infrastructure, are also used in encrypting data [9].

- Data Erasure:

There will be times when businesses need to permanently delete data from their systems because they no longer need it. Data erasure is a practical method for managing data security that reduces risk and responsibility in the event of a data breach [10].

- Data flexibility:

By making backups or copies of their data, organizations can lessen the risk of inadvertent data loss or destruction. Data backups are essential for securing information and guaranteeing its availability at all times. This will ensure that the firm can restore a prior backup in the event of a data breach or malware attack.

- Data Masking:

Data masking allows an organization to cover up and replace particular characters or numbers to conceal data. By using this kind of encryption, the data is rendered worthless if a hacker steals it. Only someone with the code to decode or swap out the masked characters may decipher the original message.

2. DISCUSSION

2.1 Data Security solution:

To safeguard their vital assets, businesses all over the world are making significant investments in information technology (IT) cyber security capabilities. The methods for incident detection and reaction to protecting organizational interests have three elements in common people, processes, and technology. This is true regardless of whether an enterprise requires to guard a brand, intellectual assets, and customer data or to provide control systems for key infrastructure. Micro Focus makes the security of sensitive data in even the most complicated use cases simple by utilizing cutting-edge data encryption, tokenization, and key management to secure data across apps, transactions, storage, and big data platforms.

- Cloud data security – A platform for data protection that enables you to go safely to the cloud while securing data in cloud apps.
- Data encryption – Solutions for data protection using tokenization in business, cloud, mobile, and big data settings.
- Hardware security module - Hardware encryption module that protects financial data and complies with regulatory standards.
- Key management -- Data protection and sector regulation compliance software.
- Enterprise Data Protection – the solution that adopts an enterprise data protection strategy that is data-centric from beginning to finish.
- Payment’s security- For retail payment transactions, the solution provider’s complete point-to-point encryption and tokenization, enabling PCI scope reduction.
- Big Data, Hadoop, and IoT data protection – Including Hadoop, Micro Focus Vertica, Teradata, and other Big Data systems, the solution safeguards delicate data in the Data Lake.
- Mobile App Security - securing critical data in native mobile apps while ensuring end-to-end data security.

- Web Browser Security - secures sensitive data gathered at the browser, starting when a user inputs credit card or other personal information, and maintains it secure across the ecosystem until it reaches the trusted host destination.
- E-mail Security – Solution that offers end-to-end encryption for email and mobile messaging, maintaining the confidentiality and security of personally identifiable and personal health information.

2.2 Data security vs data privacy:

The difference between data that may be shared with third parties (non-private data) and information that can then be shared without third-party companies is known as data privacy (private data). To enforce data privacy, there are two key considerations.

- Access control: making certain that everyone attempting to access the data is verified to verify their identity and authorized to access just the data they are permitted to access.
- Data protection: guaranteeing that, even if unauthorized individuals get access, they are unable to read or harm the data. Data loss prevention techniques restrict customers from sending sensitive data outside the company via data encryption, which stops anybody from reading data without a secret encryption key.

Data privacy and data security frequently intersect. A company's data security strategy includes the same safeguards employed to secure data privacy. The fundamental distinction is that whereas data security mostly focuses on defending against the hostile activity, data privacy primarily focuses on maintaining data confidentiality. Encryption, for instance, can be enough for privacy protection but insufficient for data security. By wiping the data or encrypting it twice to restrict access by authorized individuals, attackers might still wreak harm.

2.3 Biggest Data Security Risks

Organizations must contend with a security threat landscape that is becoming more complicated as more skilled attackers conduct cyberattacks. The following are some of the major threats to data security.

- Accidental Data Exposure: Many data breaches happen because employees unintentionally or carelessly reveal critical information, rather than as a consequence of hacking. Because they are unaware of their company's security regulations, employees might easily mishandle or lose information, share it with the incorrect person, or provide access to it.
- Phishing Attacks: In a phishing scam, a computer hacker sends communications that seem to be from a reliable sender—typically by email, SMS, or instant messaging apps. Malicious links or attachments in messages direct users to websites that are spoofs or where the attacker can steal their financial information or install malware. These assaults may also enable an attacker to enter corporate networks or compromise user devices. Social engineering is a tactic used by hackers to trick victims into divulging private information

or login passwords to privileged accounts. Phishing assaults are sometimes combined with this technique.

- Malware: Attacks using email and the internet are the most common ways that malicious software is disseminated. Attackers infect PCs' personal computers and business networks with malware by taking advantage of flaws in their software, such as web browsers or web applications. Serious data security incidents including data theft, extortion, and network damage can be caused by malware.

3. CONCLUSION

Data security refers to safeguarding digital information, such as that included in a database, against nefarious entities and uninvited human behavior, such as a cyberattack or data breach. The author of this research put equal emphasis on the concerns of data quality and security. Both of them have issues as a result of the difficulties presented by the setting of data security. It is assumed that in addition to being used to create quality systems, the solutions offered to address the issues of high volume, heterogeneity, and trustworthiness of data would also be utilized to create security ones. The conflicts that could exist have been highlighted by the author, making it more difficult to apply these systems and necessitating the search for fresh remedies. Thus, the implementation of a safe procedure to evaluate and enhance Data security will be the main emphasis of our future work.

REFERENCES:

[1] P. B. Lowry, T. Dinev, and R. Willison, “Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda,” *Eur. J. Inf. Syst.*, 2017, doi: 10.1057/s41303-017-0066-x.

[2] T. Xin and B. Xiaofang, “Online banking security analysis based on STRIDE threat model,” *Int. J. Secur. its Appl.*, 2014, doi: 10.14257/ijsia.2014.8.2.28.

[3] H. Stewart and J. Jürjens, “Data security and consumer trust in FinTech innovation in Germany,” *Inf. Comput. Secur.*, 2018, doi: 10.1108/ICS-06-2017-0039.

[4] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, “Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues,” *IEEE Access*, 2018, doi: 10.1109/ACCESS.2018.2820162.

[5] P. R. Kumar, P. H. Raj, and P. Jelciana, “Exploring Data Security Issues and Solutions in Cloud Computing,” 2018, doi: 10.1016/j.procs.2017.12.089.

[6] M. La Torre, J. Dumay, and M. A. Rea, “Breaching intellectual capital: critical reflections on Big Data security,” *Meditari Account. Res.*, 2018, doi: 10.1108/MEDAR-06-2017-0154.

[7] Y. Fernando, R. R. M. Chidambaram, and I. S. Wahyuni-TD, “The impact of Big Data analytics and data security practices on service supply chain performance,” *Benchmarking*, 2018, doi: 10.1108/BIJ-07-2017-0194.

[8] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, “Data Security and Privacy in Cloud Computing,” *International Journal of Distributed Sensor Networks*. 2014, doi: 10.1155/2014/190903.

[9] K. M. Hackett, M. Kazemi, and D. W. Sellen, “Keeping secrets in the cloud: Mobile phones, data security and privacy within the context of pregnancy and childbirth in Tanzania,” *Soc. Sci. Med.*, 2018, doi: 10.1016/j.socscimed.2018.06.014.

[10] T. Bhatia and A. K. Verma, “Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues,” *J. Supercomput.*, 2017, doi: 10.1007/s11227-016-1945-y.