Partners Universal International Research Journal (PUIRJ)
Volume: 01 Issue: 03 | July-September 2022 www.puirj.com

Data Sharing Made Easy by Technology Trends: New Data Sharing and Privacy Preserving Technologies that Bring in a New Era of Data Monetization

Dr. A. Shaji George[1], A.S. Hovan George[2]

[1]Director, Masters IT Solutions, Chennai, Tamil Nadu, India.
[2]Masters IT Solutions, Chennai, Tamil Nadu, India.

Abstract - *Soon, innovative technologies will facilitate data exchange processes between organizations without compromising privacy. Organizations are increasingly using copious amounts of external data as they extract more value from sensitive data. This can open new possibilities for data-driven decision making. Business models and products are developed through the secure sharing of data across ecosystems and value chains. Earliest days of the COVID-19 pandemic, researchers, health authorities and drug manufacturers accelerated drug and vaccine development by combining clinical data on a common platform. As a result of these data sharing protocols, drug manufacturers, government agencies, hospitals and pharmacies have jointly implemented a comprehensive immunization program that prioritizes efficacy and safety and protects intellectual property. The purpose of this article is to explain how modern technologies enable innovative business models and products by simplifying the mechanics of data-sharing across and between organizations while simultaneously maintaining privacy.*

Keywords: Fully Homomorphic Encryption, FHE, COVID-19 pandemic, partially homomorphic encryption, PHE, AI, ML, Machine Learning, Data-Sharing, privacy preserving.

1.INTRODUCTION

With the development of data-sharing technologies, it is now possible to sell and purchase potentially important data assets through extremely effective cloud-based marketplaces [1]. This data and a range of privacy preserving technologies, like FHE (fully homomorphic encryption) as well as differential privacy, enable users to communicate and calculate encrypted data without first decrypting it. It allows for the maintenance of personal privacy and security while exchanging data—the best of all scenarios. A promising emerging trend has resulted from all of this. New business model and the opportunities are emerging from the storage of confidential data lying idle on servers worldwide due to the privacy or regulation concerns [2]. In the extremely near future, more organizations will explore ways to build seamless, secure data-sharing opportunities that could help them generate revenue from their own data assets and achieve business objectives using other people's data. In spite of its early stages, data sharing is on the rise. Increasingly, global analytics and data decision-makers are using external data. Furthermore, the global FHE (fully homomorphic encryption) market is growing on its own. At present, most of the FHE explorations are taking place in the health care as well as finance sectors[3].

2.BRIEF OVERVIEW OF HOMOMORPHIC ENCRYPTION AND ITS ADVANTAGES , USES,AND TYPES

The term "homomorphic" derives from algebra and means "a structure-preserving map between two algebraic structures (it could be two groups, two rings, or even two vector spaces). Therefore, homomorphic encryption can simply be understood as a kind of encryption that enables users to perform binary operations on encrypted data with not ever having to decrypt it. This encryption allows for the encryption and outsourcing of information for processing to cloud services and environments without giving any third parties access to raw information[4].

Homomorphic encryption has the biggest advantage of being highly privacy-friendly if used correctly. In today's world, we must first decrypt encrypted data if we wish to perform mathematical operations on it. To send the data back, we have to make our necessary computations and encrypt the data again[5]. The problem arises when the encrypted data is extremely sensitive, and we do not want other services to access it. This is where homomorphic encryption comes in. The process of identifying whether a patient has a condition would be more practical if the system or service processed medical information. It is likely that the data we would be sharing includes highly sensitive medical history information. To ensure that this information is not accessible to others, other than authorized personnel, we want to ensure that no one else will have access to it.

Here, homomorphic encryption is used to process the required computations on the encrypted data, returning the diagnosis result without knowing which information has been processed. Here is the next attempt at describing: What is the goal of homomorphic encryption? If one shares sensitive information on any platform, their privacy is easily compromised. Furthermore, being able to modify and operate on data while they are still encrypted ensures the privacy of the data, which is important in today's digital world[4].

Next, let us examine homomorphic encryption types. Homomorphic encryption can be classified into the following types: 1. An infinite number of operations can be executed for ciphertext with PHE-(partially homomorphic encryption). Addition or multiplication is the only operation that can be performed here. In addition, they are much easier to design and very useful in one-arithmetic-operation applications. 2. A SHE-(somewhat homomorphic encryption) allows addition and multiplication to occur concurrently, but only a limited number of times. 3. FHE (fully homomorphic encryption) allows additions and multiplications on the ciphertext an infinite number of times and also supports arbitrary computations. FHE, or Fully Homomorphic Encryption, would be the best, but it's not exactly the case. Its major disadvantage is its poor speed as well as storage efficiency compared to plaintext encryption[5].

The Paillier cryptosystem was created by Pascal Paillier in 1999 [4]. As an additively homomorphic system, the Paillier Cryptosystem is inherently PHE-(Partial Homomorphic Encryption). Multiplication between two ciphertexts is not supported, only addition. Additionally, plaintext numbers can only be add or multiplied with ciphertext numbers. Moreover, the calculation using the Paillier Cryptosystem occurs while data encrypted. It is also possible to verify the integrity of the result by decrypting it using the private key each time. In conclusion, homomorphic encryption looks like a dream regarding data privacy and protection, but its deficient performance and excessive costs keep out of commercial and production settings. However, there have been major improvements in terms of speed lately. The pace of adoption now suggests that small commercial integrations will be seen within a few years[4,5].

3.THE IMPORTANCE OF FULLY HOMOMORPHIC ENCRYPTION

Data and personal information are being shared more widely than ever before, and users are often the ones sharing the information. In exchange for convenience and improved services, users share their data. providing the personal accounts remain untouched. For most people, giving up personal information is necessary to interact in the digital world, whether at work or in everyday life [6]. It is common for sensitive data to be encrypted before being shared. Data that is encrypted is useless to hackers and thieves because it is converted into complex code, or ciphertext. Humans cannot read such data, which is a good thing. When data is encrypted, it is protected during storage or transmission, but when the data is needed, it must be decrypted [7].

A window of opportunity is provided here, making the data vulnerable to cyber criminals, privacy violations, and other misuses. This problem is being addressed by technology companies with Fully Homomorphic Encryption (FHE), which is transforming the security paradigm. Fully homomorphic encryption allows for the use of AI and machine learning on data without exposing additional private information. In the hybrid cloud era, FHE will unlock new opportunities for business security. By processing regulated and sensitive data, FHE will enable a wider enterprise's adoption of hybrid cloud platforms, especially in industries with high levels of regulation such as finance and healthcare. Similarly, FHE could affect mergers and acquisitions, where due diligence could be performed without compromising account holders' privacy. Even airlines, hotels, and restaurants could use FHE to offer packages and promotions without disclosing details of closely held customer data. pushing forward on this new frontier of security. Data security, privacy, and client trust are all protected simultaneously[8].

4.DATA -SHARING IN ACTION CAN BE SEEN IN THE FOLLOWING EXAMPLES:

Aggregated data is used to reach common goals. Companies can collaborate with competitors in the same market segment to reach goals they both want to reach, like learning more about their customers or finding patterns of fraud in the industry.

Reduce costs and increase efficiency. Data providers no longer have to develop (APIs), provide hardware, and maintain enterprise databases. Click the button to access an anonymous and controlled data stream. When AI and (ML)machine learning are used in business, using encrypted data makes them safer and makes compliance audits easier.

collaborating with a broader range of researchers. By sharing fundamental or early-stage discoveries without jeopardizing a hard won competitive advantage, important research initiatives can be accelerated.

intellectual property protection. In the public cloud, sensitive data, like the data used to train AI, can be more protected.

Encrypt data in transit. Multiple actors are rapidly sharing sensitive data in robotic surgery, high-frequency trading, as well as smart factory manufacturing. FHE allows users to rapidly access sensitive data without encryption.

The possibility of monetizing data by sharing and aggregating data can give startups a competitive edge. This is a motivating concern in all markets today. New entrants to the data sharing ecosystem will be surprised to learn that competitors on the same platform use their data resources much more efficiently. It is at this moment that many organizations are trying to become the best based on data and artificial intelligence [9].

5.DATA TREND-THE DATA SHARING REVOLUTION

The data sharing revolution gives organizations secure access to more data, both inside and outside the ecosystem. Achieving this potential requires

managing data differently. This time, data must be managed through the integration of innovative technologies and technologies that free information assets from traditional privacy and security constraints. There are three main dimensions to current data trends: privacy, convenience, and functionality [9].

Sharing and Prosperity: New Business Models and Opportunities

business model can be developed based on shared data. As the data sharing trend evolves, more organizations are engaging in "data collaboration" to solve common problems and find revenue, operational, and research opportunities. Organizations can also securely share data with third-party data management service providers to streamline data management processes and reduce costs. Data sharing can lead to the following opportunities:

The vertical industry market. The fiercest competitors often face familiar challenges that they can solve together. Take a supplier in the food industry as an example. Anonymizing and analyzing confidential sales and shipping data together can solve the mystery of supply and demand. Anonymized credit data can be combined to create interbank credit risk assessment systems for developing countries. Biggest Opportunity: What if pharmaceutical researchers and doctors could collect data to speed up the development of life-saving innovations while working in a safe environment.

Providers of data streamline delivery processes. Real-time market and logistics data can be acquired at the click of a button on the data sharing platform. Providers no longer need to provide APIs or send files.

AI model training can be done by someone else. In many cases, AI designs are considered an extremely sensitive form of intellectual property. Because they are generally portable, they also pose a high security risk. Therefore, many organizations create their own simulations. Fortunately, encryption technology can change that. As long as the simulation data is protected, AI simulations and training can be sent to third parties in a safe way.

Value chain partners. Many producers and retailers buy customer data from a third party intermediaries, but as often happens, there is not sufficient good-quality data to really be effective. What happens when value chain partners, from manufacturers to suppliers to marketers, combine customer data[9].

6.EXTERNAL DATA CAN BE EASILY ACQUIRED WITH THE CLICK OF A BUTTION

A cloud based data sharing platform allows the user to effortlessly share, purchase, and sell data between organizations. Typically, these highly virtualized, high-performance data stores allow subscribers to control, manage, and customize their data by paying for a service. Data may also be protected using a "clean room" provided by the platform, a secure space where data assets can be pooled for analysis [10]. As a final step, subscribers can aggregate data access and sell it to other subscribers. Data buyers can choose from multiple views based on the buyer's market, product, or research needs. Sharing as a service has proven effective in other popular areas of information and content sharing, such as music file sharing and social networking. The provider provides the platform, and the customer provides the content (data)[11]. AWS, Azure, Google, and Salesforce are among the hyperscale cloud providers competing for their place in the data market. It's currently a gold rush with startups like Databricks, Datarade, Dawex, and Snowflake. It's really promising. With the growth of data, digital transformation will lead to a revolution where there is a greater demand for external data. In addition to informing executive decisions, data is now an important business asset that can be traded, bought, and sold. Ultimately, the platform that makes this exchange easiest and most efficient can become standard for data sharing across industries.

As more organizations look for ways to monetize and grow their data assets, the use cases and best practices for data sharing are growing. Some examples: In the initial stages of the (COVID-19)pandemic, intensely competing global pharmaceutical companies looked for ways to share data from preclinical studies. Administrators of the COVID-19 vaccine have used a centralized government platform to share immunization and test data with the public health authorities[10,11]. Investment managers at global financial services companies collect and analyze real-time data from the back office, middle office, and front office. Consequently, the opportunity to share investment data with customers takes minutes instead of months.

The future development of the data sharing platform market is still expected. In addition to consolidation and standardization, more platform markets may emerge. Personal data marketplaces can partner, and open marketplaces can emerge voluntarily to meet unique requirements. Regardless of what shape the data market ultimately takes, we expect the gold rush to continue, especially as vendors develop robust safety and more organizations register these platforms, increasing the amount of external data are available for consumption [11].

7.DATA SHARING WITHOUT COMPROMISING PRIVACY

Sharing data increases its value. However, historical data privacy policies and competitive privacy requirements have limited the realization of this value. Privacy computing (or secret computing) is poised to free organizations and their data from the constraints of privacy. Approaches like FHE, differential privacy, and characteristic encryption can be used to share data without giving up privacy[9]. Privacy technologies allow competitors to collaborate. There are many financial institutions competing in various sectors of financial services. Even if the company competes for customers, companies can work together to detect the risk of overconcentration, complex patterns of fraud, or financial crime. Consider a business that is complementary, but not competitive, in an industry like travel [10]. Airlines, hotels, and car rental companies can take advantage of data sharing by adding information to corporate marketing and discount campaigns. Participating companies take care of each other's behavior and customer behavior to provide more value to end users. However, everyone has an obligation to protect customer data. It can be a computer that protects privacy and makes it easier for businesses to work together and talk to each other. There are currently four challenges which are slowing down progress in privacy. These methods require new software tools and modifications. Fully using and maintaining these tools can take a lot of time and effort for an already busy team. In some cases, privacy can slow down speed and performance, making real-time analysis and data distribution difficult. When data is in the hands of others, it is difficult to manage and monitor data usage, creating privacy and compliance issues. Before personal computing can reach its full potential, there are some legal issues that need to be dealt with. These include privacy and who owns the data. However, the personal computer offers a variety of features and usage scenarios [12].

8.POLICYMAKERS MUST ACT ON THE BASIS OF THESE RECOMMENDATIONS

The purpose of privacy regulations is to empower consumers by giving them the ability to share, control, and protect their personal information. This regulation requires responsible use of data and a fair exchange of information. A full framework for understanding the privacy tensions that come with new digital technologies and types of data strategies led to a number of recommendations.

9.THERE IS A NEED TO ADDRESS THE EVOLUTION OF DIGITAL TECHNOLOGY

Given the rapid development of digital technologies, privacy regulations must keep pace with these

developments. Privacy regulations may not be appropriate for the future, but lawmakers can protect consumers more broadly by regulating data sharing that is fundamental rather than specific technological methods. These rules prevent firms from bypassing the restrictions with technologically advanced solutions. Even the most comprehensive regulatory mechanisms can be challenged by new digital applications such as deep counterfeiting, disinformation, and advertising ecosystems. To avoid regulatory obsolescence and business violations of regulatory frameworks, laws and protections should be set in a way that has nothing to do with technology. It is important for regulators to examine the implications of their proposals, but they should also work closely with firms to understand how they will be implemented. Identifying violations and requiring high-level compliance are not sufficient monitoring efforts. If technological developments are too rapid to be subject to specific regulation, policymakers need to keep an up-to-date understanding of recent technology developments.

10. CONCLUSIONS

Companies are using an increasing amount of external data as they derive more value from sensitive data. Advances in data sharing technologies now make it possible to buy and sell potentially valuable data assets through cloud-based marketplaces. Data providers no longer need to develop APIs, provide hardware, or maintain corporate databases. Critical research initiatives can be accelerated by sharing basic or early discoveries without compromising intellectual property protection. Sensitive data, such as data that is used to train (AI)artificial intelligence, can be better protected in the public cloud. Long-term relationships with key stakeholders require significant investment in digital technologies. Businesses can gain access to large amounts of data through digital technology, providing a number of benefits. Research and actionable insights from businesses, consumers, and regulators need to be integrated into a comprehensive framework. There will be effects on consumer privacy and the tension between sharing practices and making money off of data. The data sharing revolution gives organizations secure access to more data, both inside and outside the ecosystem. Real-time market and logistics data can be linked into the data exchange platform at the click of a button. Private data markets can become subsidiary, and open markets can emerge voluntarily to meet unique requirements. The cloud-based data sharing platform allows users to easily buy, share, and to sell data between organizations.

REFERENCES

[1] "Fully Homomorphic Encryption Market – Global Industry Trends and Forecast to 2028 | Data Bridge Market Research." Fully Homomorphic Encryption Market – Global Industry Trends and Forecast to 2028 | Data Bridge Market Research, www.databridgemarketresearch.com/reports/global-fully-homomorphic-encryption-market.

[2] "Maximizing Collaboration Through Secure Data Sharing | Accenture." Maximizing Collaboration Through Secure Data Sharing | Accenture, 1 Oct. 2019, www.accenture.com/us-en/insights/digital/maximize-collaboration-secure-data-sharing.

[3] "Homomorphic Encryption for Data Privacy - TripleBlind." TripleBlind, 26 May 2022, tripleblind.ai/homomorphic-encryption-for-data-privacy.

[4] "What Is Homomorphic Encryption?" Experfy Insights, 4 Oct. 2019, resources.experfy.com/bigdata-cloud/what-is-homomorphic-encryption.

[5] "What Is Homomorphic Encryption?" freeCodeCamp.Org, 26 Apr. 2022, www.freecodecamp.org/news/introduction-to-homomorphic-encryption.

[6] Marr, Bernard. "What Is Homomorphic Encryption? And Why Is It So Transformative?" Forbes, 15 Nov. 2019, www.forbes.com/sites/bernardmarr/2019/11/15/what-is-homomorphic-encryption-and-why-is-it-so-transformative.

[7] Dr. A.SHAJI GEORGE, & A.S.HOVAN GEORGE. (2022). Potential Risk: Hosting Cloud Services Outside the Country. International Journal of Advanced Research in Computer and Communication Engineering, 11(4), 5–11. https://doi.org/10.5281/zenodo.6548114

[8] "Fully Homomorphic Encryption Content Solution." IBM Z Content Solutions | Fully

Homomorphic Encryption, www.ibm.com/support/z-content-solutions/fully-homomorphic-encryption.

[9] "Data-Sharing Technologies Made Easy | Deloitte Insights." Deloitte Insights, 7 Dec. 2021, www2.deloitte.com/us/en/insights/focus/tech-trends/2022/data-sharing-technologies.html.

[10] Solution, Snowdrop. "New era Of Data Monetization: Advances In Data Sharing Technologies Made It Easy To Share Data While Preserving Security And Privacy – Snowdrop Solution." New Era Of Data Monetization: Advances In Data-Sharing Technologies Made It Easy To Share Data While Preserving Security And Privacy – Snowdrop Solution, 13 Jan. 2022, www.snowdropsolution.com/big-data/new-era-of-data-monetization-advances-in-data-sharing-technologies-made-it-easy-to-share-data-while-preserving-security-and-privacy.

[11] "What Is A Data Platform? | MongoDB." MongoDB, www.mongodb.com/what-is-a-data-platform.

[12] "Consumer Data Protection and Privacy | McKinsey." McKinsey & Company, www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative.