Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2021, 8(7):265-273**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Application of Big Data Platform for Secure Sensitive Data Sharing

Kartheek Pamarthi

Kartheek.pamarthi@gmail.com

Abstract: Big data has been utilised by a variety of businesses in order to simplify the delivery of products and to improve consumer insights by utilising predictions made possible by technologies such as artificial intelligence. Big data is a field that focuses primarily on the extraction and systematic analysis of big data sets with the goal of assisting businesses in identifying patterns using this information. With the advent of Big Data, numerous businesses are able to expand their capacity to manage enormous client datasets and allow growth in a variety of functional areas. Many software corporations are increasing their investments in companies that specialise in data management and analytics as a result of the increased need for information management specialists brought about by big data. The administration of large data is, however, vulnerable to the problem of data protection or privacy concerns. In this article, some of the most significant problems regarding the application and utilisation of Big Data are discussed. These concerns pertain to the difficulties associated with maintaining the confidentiality and safety of data that is held on technical equipment. A number of the ongoing research projects that are being carried out with the purpose of resolving concerns regarding privacy and security in relation to Big Data are also discussed in this paper.

Keywords: Big data, Security, Data sharing

Introduction

The "Big Data" that could cripple a company is the data that is both massive and growing at an exponential rate [1]. It compiles data streams from numerous separate sources that are large, varied, and multi-format. Many people believe that Big Data has five traits, which are called the "five V's." Some of these features are valence, variety, loudness, speed, and veracity [2]. A new overlapping sixth V: value has been added to the method for massive data sets, as seen in Figure 1.

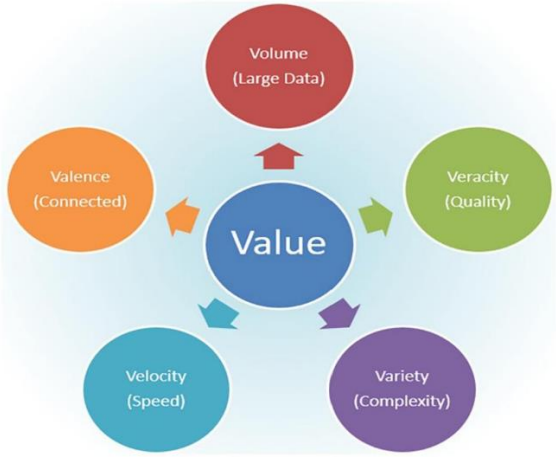

Figure 1. Big Data: The Six Vs.

Big Data, indicative of the sheer amount of data, is the defining feature of large data. This results from the expansion of storage area networks and massive data centres. There is a broad variety of dimensionalities and data heterogeneity as a result of the vast amounts of huge data. Given this, attempting to decrease the quantity is crucial for effectively analysing huge figures [3]. Avoiding the utilisation of resources for lateral processing and storage necessitates treating massive data streams online. Another key feature of Big Data is how quickly it processes information. Speed, which is related to the frequency of data streams, needs to be reduced for huge data management to be effective. One such example is the observatory for solar dynamics, which daily produces data equivalent to around one terabyte. Only after reduction and summary can such rapid data be envisioned for analysis. Big Data is afflicted by the so-called "curse of dimensionality." Rephrasing this another way, we need to successfully reduce millions of dimensions, which comprise variables, traits, and attributes [4], in order to find the most knowledge patterns.

For example, Internet user activity profiles are both comprehensive and sparse, yet they include millions of potentially useful phrases and URLs. Similarly, an individual's high-performance genetic sequence adds to the high dimensionality of data while simultaneously increasing its volume and speed. The amount and variety of massive data sets are increasing at an exponential rate, and many different things are adding to this trend. Furthermore, Big Data is used in many nations to provide services to numerous businesses, such as manufacturing, distribution, marketing, healthcare, and public sector activities [5]. For example, businesses like stores are collecting vast amounts of customer sales data in their databases. Companies are concentrating on enhancing their financial and logistical services, while individuals are sharing a lot of information about sales prices and products on social media. The sheer amount and variety of data, both structured and unstructured, is one of the many obstacles that big data inevitably brings. Improved instructional and learning processes, new forms of assessment for students, and better decision-making and educational leadership are all outcomes of using Big Data in HE researches [6]. Potentially game-changing effects may result from these novel analytics methods. Customers in the retail sector, for example, sometimes employ Big Data Analytics to learn which products are in season and which regions will have the highest demand. Despite its many advantages, big data analytics has sparked new worries about data security [7].

This is in addition to the incredible business prospects that it currently presents. The discovery of anomalies and fraudulent activity can be accomplished through the utilisation of Big Data analysis as a foundation for safety analytics. The analysis could be conducted in a geographically dispersed environment because data transmissions between organisations are not always reliable. With the right infrastructure in place, researchers may investigate massive volumes of data using techniques like information mining and statistical analysis, made possible by the widespread storage of diverse types of data in numerous systems.

The collection and storage of enormous volumes of data is one aspect of the situation. However, on the other hand, it is more challenging to protect massive amounts of data from being accessed by unauthorised parties [8]. Another crucial point is that cyber threats and attacks are forever open season because of the cyber world.

The term "cybersecurity" stands for the strategies, instruments, and procedures that are utilised in the fight against cyber-attacks and cyber-based dangers. Traditional security solutions were not especially effective when it came to detecting and combating fraud, cyber-attacks, and other threats. Hackers with advanced cyber capabilities can readily breach a company's defences and steal confidential information, including trade secrets, customer databases, and financial details. There has been a meteoric rise in the use of IoT-based applications in modern society. Academics studying the Internet of Things (IoT) have made user data security a hot issue [9].

Research conducted in the Internet of Things Cloud has resulted in the development of efficient security protocols that provide comprehensive frames with software characteristics of critical significance. These protocols are designed to guarantee that data flows between devices are both secure and accurate. There is a daily increase in the number of people who use the internet as the cost of using the internet continues to decrease. This is leading to an increase in the amount of data that is being transferred across the Internet [10].

Literature Review

Currently, social networking is experiencing a daily expansion that is occurring at a quick pace. Registrations for social media networks are made by millions of people each and every day. Many people use social media for many reasons, such as business, learning, and enjoyment [11]. One of the greatest accomplishments of the past

few years is the proliferation of small, powerful wireless devices that can establish connections across a broad range of wireless networks with different link-level properties.

Transferring data from one place to another is a crucial part of the software industry's technological landscape. Since all technologies rely on data in some way, software is fundamental to all technology [12]. Sharing information and the ability to upload, read, download, and understand material is the primary goal of almost all social networking services (SNS). A knowledge-based society and information can be fostered through sharing information for many reasons, such as but not limited to: attracting like-minded individuals, increasing social capital, strengthening individual relationships, attracting attention, and so on. Also, as previously stated, a lot of people use it for different things, but some bad actors, like hackers, create false profiles and utilise these platforms for their own illicit ends. They make a phoney profile with a phoney photo so they may impersonate someone else. False information dissemination, other forms of deceit, and other illegal behaviours are among the many things they do with these profiles [13]. Cybercrime is on the rise in today's IT industry, outpacing the effectiveness of existing cybersecurity measures. [14] Computer systems can be vulnerable to attacks due to a variety of reasons, including improper setup, inexperience, and a lack of available approaches.

As a result of the growing threats posed by the internet, there is a pressing need for increased advancement in the development of cybersecurity strategies. Threats posed by the internet have considerably increased. The rate at which safety dangers are occurring and the requirement to manage them is becoming an increasingly challenging situation. Learning by machine is one of the most cutting- edge approaches of detecting criminal activity on the internet. It is possible to make use of machine learning techniques in order to circumvent the limitations that are associated with conventional detection methods [15]. There is a growing demand for machine learning applications in a variety of fields, including education, healthcare, business, and cybersecurity, among others.

The major objective of this article is to discuss data security and protection issues and provide ways to find weaknesses. Big Data Analytics raises a lot of privacy and security issues, which are addressed in this article. This study provides a synopsis of the different machine learning approaches, as well as the data sets normally used for security purposes.

Although the importance of cyber security cannot be overstated, there are still breaches and obstacles to overcome. Additionally, this work sheds light on the substantial challenges and limitations that are associated with the utilisation of cybersecurity [16]. Data privacy is an issue with Big Data. Quick and efficient algorithms for Big Data security intelligence are the focus of the research community's efforts. Big Data, computer science, and the proliferation of commercial applications are the frameworks within which these endeavours are being carried out. The primary goal of this undertaking is to ensure a safe environment that is not accessible to unauthorised individuals [17].

Security analysis will transform these technologies by collecting and analysing massive amounts of data from both internal and external sources, including vulnerability databases. The data will be collected and analysed to achieve this. Provide a holistic perspective of the security data and conduct analysis on the data in real-time. While trying to define "Big Data Tools," bear in mind that analysts and architects of systems still require system education [18]. The study of big data has enormous promise for improving every facet of business, creating game-changing innovations, and helping people in many ways with their privacy concerns. However, before starting to employ analytics, organisations should examine the concerns concerning privacy and security while implementing Big Data Analytics [19].

During Bertinoet and Ferrari's meeting, the fundamental concepts and processes for the protection of enormous amounts of data and their confidentiality were discussed. Furthermore, they brought attention to crucial research issues that must be resolved to ensure complete data security and privacy inside the Big Data framework [20].

A computing paradigm that safeguards your privacy was invented in [21], and it functioned by requiring you to download expensive cloud activities. On the client side, they have developed a method that is very scalable for encryption and decryption, while the cloud is responsible for the processing of any significant actions. In comparison to the conventional method of deep calculation, their approach improves preparation efficiency by a factor of 2.5 while maintaining the confidentiality of personally identifiable information. To help preserve people's privacy in video streams, Brki'c suggested a machine vision pipeline that takes into account the inherent value of obscured faces and unidentified data [22].

In his work, [23] makes the point that Big Data provides individuals with both comfort and the ability to maintain their privacy. In this brief review, he discusses the challenges that are presented by the collecting, storage, and interpretation of big data. Because of this, verifying Big Data's veracity is crucial, and we must also address the limitations of current data security technology and the legal issues surrounding data protection. Bertino and Ferrari express worry in their research on the dangers of new data collecting and processing methods to Big Data. In this work, they look at some of the basic ideas and approaches that can be used to protect Big Data against these kinds of dangers. Along with this, they brought attention to the research gaps that must be filled before we can address the growing amount of Big Data with solutions that are both secure and private [24].

For the safe transfer of confidential information, a Big Data Platform provides a three-pronged approach. An information security system is necessary for the purpose of renting and issuing sensitive data on a big data platform that is only partially trustworthy. Trustworthy submission, secure storage, riskless usage, and secure destruction are the four facets of safety challenges that must be considered while building secure channels to allow the whole life cycle of sensitive data to be utilised. For the purpose of securely sharing sensitive data on a big data platform, Figure 2 shows a methodological structure that might be utilised.

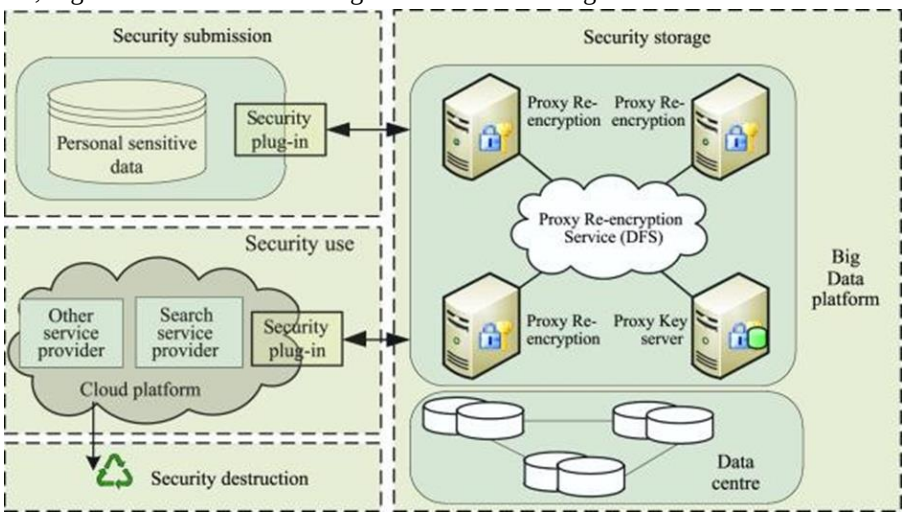

Figure 2: A Big Data Platform Security Architecture for Sharing Sensitive Information.

When submitting data to a semi-trusted big data platform, encrypting it before transmission is one of the most common and popular ways to ensure its security. Some tasks, such as encryption, decryption, and permission, can be accomplished with the help of a security plug-in. Data used by a cloud platform service provider (such a SESP) on a big data platform can be protected by downloading and using the security plug-in. Our new Heterogeneous Proxy Re-Encryption (H-PRE) framework enables seamless transitions between several types of encryption, including public-key encryption (PKE) and identity- based encryption (IBE). To ensure the security of the storage, this was done. Using H-PRE with traditional cryptography won't cause any issues. The goal is to encrypt the data that the owner uploads using cypher techniques and then decrypt it using the user's private key.

Assuming the cloud is unreliable and that decrypted plaintext will expose people's private information, we are functioning accordingly. Implementing a process protection solution based on a virtual machine monitor (VMM) and implemented through a trusted VMM layer is essential for us to bypass the guest operating system and deliver data protection directly to the user process. The new registration programme group's public keys are stored using the key management module of the virtual machine manager (VMM). During programme execution, the key management module is responsible for dynamically decrypting the symmetric key present in the main program's base. The virtual machine manager (VMM) stores all of the public and symmetric key applications in its memory. When using cloud storage for archiving, replication, and backup, data redundancy is created. To eliminate this risk and protect user privacy, it is important to implement a data destruction policy. We came up with a lease-based way to attain high degrees of security by comprehensively and controlledly destroying sensitive data and keys.

After the lease has expired, cleartext and keys are no longer present in the cloud for any reason. Following is an outline of the fundamental flow of the framework. In order to begin, companies that collect personally identifiable information should determine in advance which service providers will be required to access this data. The next step is for companies to use the local security plug-in component to submit and store encrypted data on a big data platform, which corresponds to the sensitive information. Secondly, in order to process the given data, we must utilise PRE on the big data platform. Then, in the private process space, with the help of the secure plug-in, the cloud platform service providers that need to communicate sensitive data can download and decrypt the matching data. We do this to make sure the data gets sent correctly. Finally, we employ a secure method to remove existing data from the cloud, even if it has been used. To sum up, the framework offers an effective way to protect sensitive data across its full life cycle. The data owners retain complete ownership of their property during this process. What follows is an explanation of the most crucial PRE algorithm, which employs methods for user process protection that rely on the VMM and is based on heterogeneous cipher-text transformation.

Secure Use of Sensitive Data on VMM

The private space of a user process based on a VMM

Using the private area of a user process based on a virtual machine monitor (VMM) allows us to operate an application securely in the cloud.

IaaS stands for infrastructure as a service, and we are going to suppose that some business, like a SESP, rents it in order to carry out some kind of operation. The business process cannot run on the big data platform without first extracting personally identifiable information.

A sensitive process is what we refer to as the protected programme within the big data platform that is responsible for extracting sensitive data. Figure 3 depicts a threat model of a sensitive process that happens to be running on a cloud platform. The management virtual machine monitor (VMM) and the unstable operating system layer below it provide threats to a vulnerable process, which must be protected. Bottom hardware that is rented out uses the TPM mode to guarantee that the VMM can be trusted.

In this scenario, the key management mechanism of the renter, which may be a SESP, is required to establish this relationship on the basis of trusting a VMM in order to guarantee safe operation despite the unreliable functionality of the operating system.

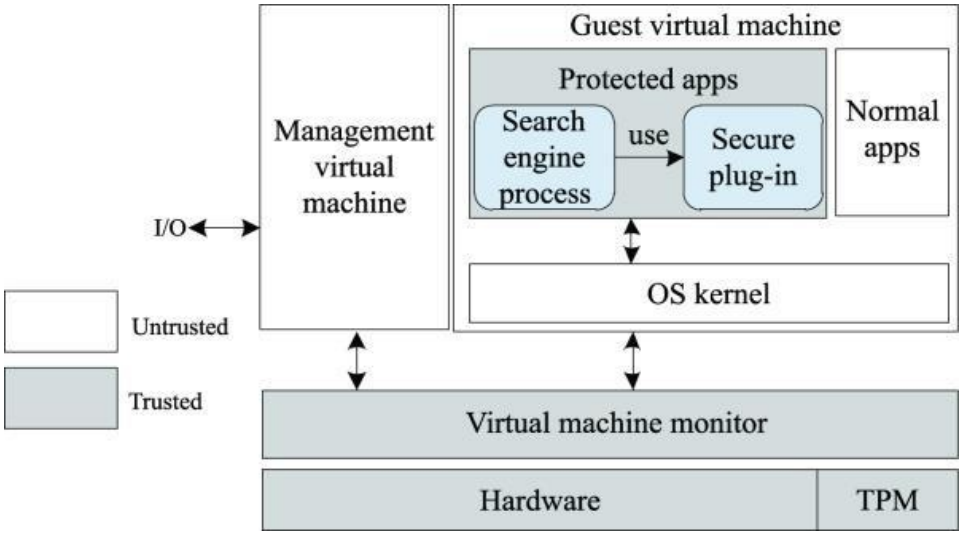

Figure 3: Cloud platform threat model for a sensitive process.

An encrypted plug-in and virtualization for service provider apps can be made to run in a private environment with the help of trusted computing and virtualization technologies.

This mode eliminates the possibility of interference from third-party programmes, including the operating system, and safeguards the confidentiality of sensitive data. Figure 4 depicts a procedure for safe functioning of the system.

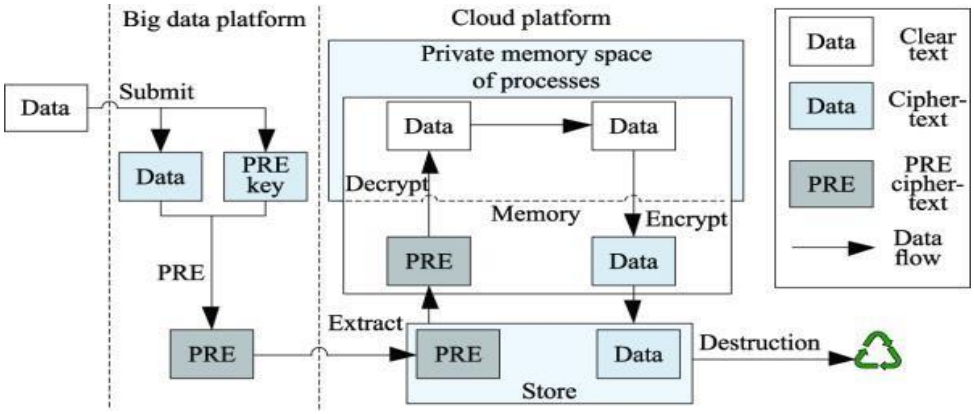

Figure 4: Safe operation process

By moving the PRE ciphertext from a large data platform to a cloud platform, operations running on the cloud can ensure the security of data in memory and on the hard disc drive (HDD).

To begin, the Virtual Machine Manager creates a private memory area that can be used to specify a virtual machine process. The operating system and other applications are unable to access the memory because the process is running in a private memory area. Memory isolation is a method that, when applied, guarantees the confidentiality and safety of data stored in memory. Furthermore, the data that is utilised and saved on the disc is composed of ciphertext. The Virtual Machine Manager (VMM) is accountable for decrypting or encrypting data while it is reading or writing data, on the other hand. Regardless of whether the user programme is now running in memory or is stored on disc, the Virtual Machine Manager (VMM) can be used to protect a combination of these two measures. This is the case regardless of whether the user programme is stored on disc or operates in memory.

Secure use of system sensitive data

By employing process protection technology based on a virtual machine monitor (VMM), we are able to circumvent the guest operating system and directly secure the user process's data. A trustworthy VMM layer is used to deploy this technology. In order to keep data secure during the whole interaction process on the cloud platform, you must do the following tasks.

(1) Establishing a credible environment and channels

The cloud platform must assess the startup programme using trusted computing technologies during the booting process. Cloud users, or SESPs, must ensure the integrity of the VMM because of this. Users of the cloud should verify the VMM's reliability on their own. After the boot process is finished, the cloud server will save the platform configuration settings, BIOS settings, and VMM measurements to the TPM chip's Platform Configuration Register (PCR). The next step is for the cloud server to verify the continued existence of the trust connection by sending a remote verification to the user. Before securely receiving sensitive data from the big data platform, the SESP must establish a reliable connection with the cloud-based VMM. Figure 5 shows the protocol that the SESP and the cloud-hosted VMM utilise for remote attestation and hand shaking.

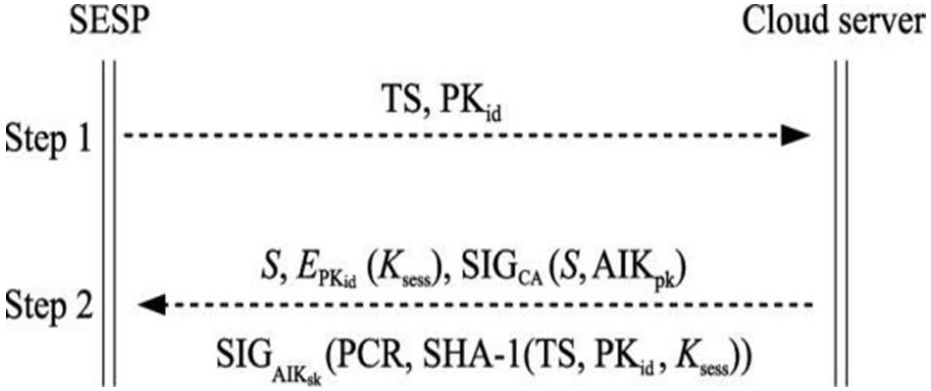

Figure 5: illustrates the remote attestation and handshake protocol between the SESP and the VMM in the cloud.

The VMM actually handles the request on the end of the cloud server. In the first step, the SESP communicates with the cloud server by sending an integrality request that includes the timestamp (TS) and the SESP public key (PKidPKid). The second step is for the VMM to use the Secure Hash Algorithm (SHA1) to compute the hashed values of TS, PKid, and Ksess. The session key is then generated. The testimony (quote) is retrieved by the VMM using the TPM private key signature. This is accomplished by executing the TPM quote instruction with the hashed value and PCR as inputs.

The certification authority (CA) certificate, Quote, and Ksess*K*sess are sent to the other side by the VMM after they have encrypted them using PKidPKid. When the SESP receives this information, it checks the value of TS, PKid, and Ksess. All communications will be safe if the values are same. Consequently, a session key is decided upon by both parties involved in the interactions. Going forward, the session key will be used to encrypt communication on both ends.

(2) Data upload and extraction Users in the cloud, also known as SESPs, retrieve sensitive information from the big data platform. We do not put our faith in the cloud. Before the SESP can use the cloud, it must encrypt the data and executable application that it uploads. The data upload and extraction methodology is illustrated in Figure 6.

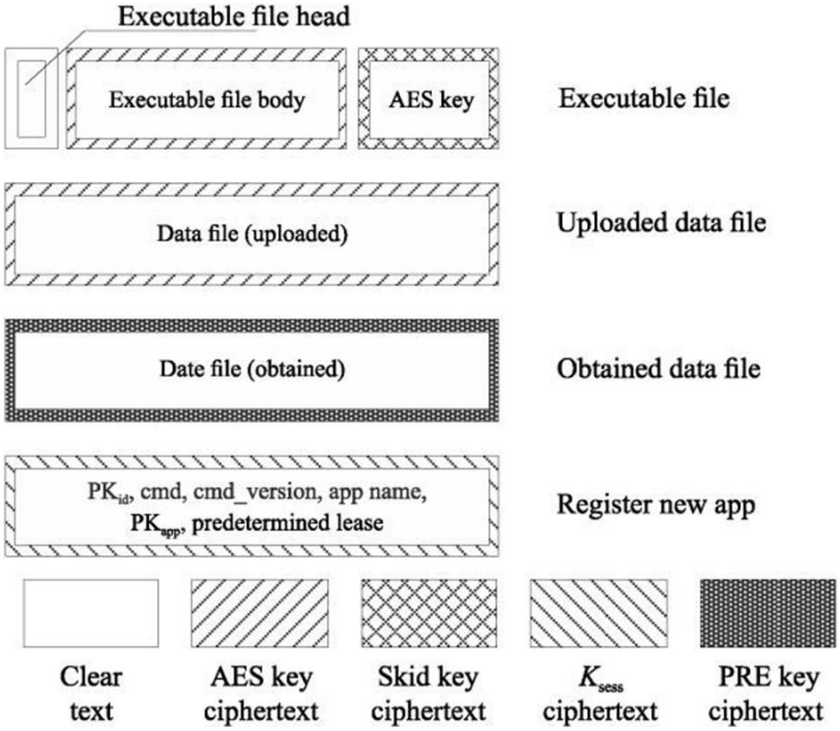

Figure 6: illustrates the technique for uploading and extracting the data

Figure 6 illustrates the utilisation of tools by the SESP to produce an AES symmetric key and two asymmetric keys, namely PKappPKapp and SKappSKapp. Subsequently, the data files and executables are encrypted using the AES symmetric key, while the AES key itself is encrypted using the asymmetric keys and added to the application files. To simplify the process of decrypting data during runtime, the information obtained from the big data platform is saved in PRE ciphertext. During the registration process, it is necessary to specify the command format for the new software. Before transmitting them to the VMM, the user encrypts the following data: PKid (Public Key Identifier), registration command, application name, public key (PKapp), and predefined lease using Ksess***W***sess (Session Key).

Lastly, the data and executable files are uploaded to the server in the cloud with an encryption key.

(3) Running the programme

As seen in Figure 4, the encryption and protection of dynamic data during programme execution on the cloud platform is comparable to the security of process memory space [18, 19, 20, 21]. While a process is running in occupied memory, no other processes or operating systems are able to access it. The Virtual Machine Monitor (VMM) mediates communication between the user process and the operating system. When the operating

system copies data from the user memory region, the VMM does the actual copying instead of the OS because the OS does not have read/write privileges. Using the corresponding AES symmetric key, the VMM decrypts data after it has been copied into the process's private memory space. Because of this, regular calculations may be performed on the data. When data is copied from the process's private memory area to an external location, the VMM encrypts it using the corresponding AES symmetric key. All user data stored on disc is now in ciphertext. To put it simply, a user process's private domain is where the VMM decrypts data from the cloud user (SESP), while the security plug- in decrypts PRE data from the big data platform.

The data is encrypted once the user process is over, and then it is deleted in accordance with the lease conditions. Thus, the user's private area serves as a middle ground in the security mechanism, protecting sensitive information while also benefiting the data owner.

Conclusions

In summary, we have suggested a structured framework for the secure exchange of sensitive data on big data platforms. The Private Space of user processes that are based on the VMM is guaranteed the secure use of plain text in the cloud platform by this framework. It also guarantees the secure submission and storage of sensitive data through the heterogeneous proxy re-encryption algorithm. The confidentiality of users' sensitive data is safeguarded to an exceptional extent by the proposed framework. Simultaneously, the data owners maintain complete control over their own data, a viable approach to reconcile the interests of the numerous parties engaged in the situation in the context of semi-trust. We will enhance the efficacy of encryption by optimising the heterogeneous proxy re- encryption algorithm in the future. Additional improvements will be implemented. Furthermore, an additional substantial endeavour that will be implemented in the future is the reduction of the overhead associated with the interaction between the numerous parties.

References

[1]. Abdulhamid, S. M., Abd Latiff, M. S., Chiroma, H., Osho, O., AbdulSalaam, G., Abubakar, A. I., & Herawan, T. (2017). A review on mobile SMS spam filtering techniques. IEEE Access, 5, 15650– 15666. https://doi.org/10.1109/ACCESS.2017.2666785

[2]. Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: Preserving security and privacy. Journal of Big Data, 5(1), 1–18. https://doi.org/10.1186/s40537-017-0110- 7

[3]. Adjei, J. K., Adams, S., Mensah, I. K., Tobbin, P. E., & OdeiAppiah, S. (2020). Digital identity management on social media: Exploring the factors that influence personal information disclosure on social media. Sustainability (Switzerland), 12(23), 1–17. https://doi.org/10.3390/su12239994

[4]. ftab, M. O., Javed Awan, M., Khalid, S., Javed, R., & Shabir, H. (May 2021). Executing spark BigDL for leukemia detection from microscopic images using transfer learning [Conference session]. 2021 1st International Conference on Artificial Intelligence and Data Analytics, CAIDA 2021, Riyadh, Saudi Arabia, pp. 216–220. https://doi.org/10.1109/ CAIDA51941.2021.9425264

[5]. Ahmed, H. M., Awan, M. J., Khan, N. S., Yasin, A., & Shehzad, H. M. F. (April 2021). Sentiment analysis of online food reviews using Big Data analytics. Ilkogretim Online, 20(2), 827–836. https:// doi.org/10.17051/ilkonline.2021.02.93

[6]. Barth-Jones, D. C. (2012). The “Re-Identification” of governor William Weld’s medical information: A critical re-examination of health data identification risks and privacy protections, then and now. https://doi.org/10.2139/ssrn.2076397

[7]. Battams, K. (2015). Stream mining for solar physics: Applications and implications for big solar data [Conference Session]. Proceedings – 2014 IEEE International Conference on Big Data, IEEE Big Data 2014, Washington, DC, pp. 18–26. https://doi.org/10.1109/BigData.2014.7004400

[8]. 8.Butpheng, C., Yeh, K. H., & Xiong, H. (2020). Security and privacy in IoT-cloud-based e-health systems-A comprehensive review. Symmetry, 12(7), 1–35. https://doi.org/10.3390/sym12071191

[9]. Cárdenas, A. A., Manadhata, P. K., & Rajan, S. P. (2013). Big data analytics for security. IEEE Security & Privacy, 11(6), 74–76.

[10]. Chandramouli, B., Goldstein, J., & Duan, S. (2012). Temporal analytics on Big Data for web advertising [Conference Session]. Proceedings – International Conference on Data Engineering, Arlington, VA, pp. 90–101. https://doi.org/10.1109/ ICDE.2012.55
[11]. Chandrasekar, Dr. C. (2018). Classification techniques using spam filtering email. International Journal of Advanced Research in Computer Science, 9(2), 402–410. https://doi.org/10.26483/ ijarcs.v9i2.5571
[12]. De Goede, M. (2014). The politics of privacy in the age of preemptive security. International Political Sociology, 8(1), 100–104. https://doi.org/10.1111/ips.12042
[13]. Dev Mishra, A., & Beer Singh, Y. (2017). Big Data analytics for security and privacy challenges [Conference session]. Proceeding – IEEE International Conference on Computing, Communication and Automation, ICCCA 2016, Greater Noida, India, pp. 50–53. https://doi.org/10.1109/CCAA.2016.7813688
[14]. Ebert, I., Wildhaber, I., & Adams-Prassl, J. (May 2021). Big Data in the workplace: Privacy due diligence as a human rightsbased approach to employee privacy protection. Big Data and Society, 8(1). https://doi.org/10.1177/20539517211013051
[15]. Farkas, C. (2014). Big Data analytics: Privacy protection using semantic web technologies [Conference session]. NSF Workshop on Big Data Security and Privacy, Texas, San Antonio, United States.
[16]. Firdausi, I., Lim, C., Erwin, A., & Nugroho, A. S. (2010). Analysis of machine learning techniques used in behavior-based malware detection [Conference session]. Proceedings – 2010 2nd International Conference on Advances in Computing, Control and Telecommunication Technologies, ACT 2010, Jakarta, Indonesia, pp. 201–203. https://doi.org/10.1109/ACT.2010.33
[17]. Florea, D., & Florea, S. (2020). Big Data and the ethical implications of data privacy in higher education research. Sustainability (Switzerland), 12(20), 1–11. https://doi.org/10.3390/su1220 8744
[18]. Gahi, Y., & Alaoui, I. El. (2019). A secure multi-user databaseas-a-service approach for cloud computing privacy. Procedia Computer Science, 160, 811–818. https://doi.org/10.1016/j. procs.2019.11.006
[19]. Gai, K., Qiu, M., & Zhao, H. (2016). Security-aware efficient mass distributed storage approach for cloud systems in Big Data [Conference session]. Proceedings – 2nd IEEE International Conference on Big Data Security on Cloud, IEEE BigDataSecurity 2016, 2nd IEEE International Conference on High Performance and Smart Computing, IEEE HPSC 2016 and IEEE International Conference on Intelligent Data and S, New York, NY, pp. 140–145. https://doi.org/10.1109/ BigDataSecurity-HPSC-IDS.2016.68
[20]. Geist, A., & Reed, D. A. (2017). A survey of high-performance computing scaling challenges. The International Journal of High Performance Computing Applications, 31(1), 104–113. https://doi.org/10.1177/109434201559708
[21]. Guo, J., Yang, M., & Wan, B. (June 2021). A practical privacy-preserving publishing mechanism based on personalized k-anonymity and temporal differential privacy for wearable iot applications. Symmetry, 13(6), 1043. https://doi.org/10.3390/sym13061043
[22]. Inbarani, H. H., & Kumar, S. S. (2015). Big Data in complex systems (Vol. 9). Springer. https://doi.org/10.1007/978-3-319-11056-1
[23]. International Standard Organization. (2011). International standard ISO/IEC information technology—Security techniques— Application security.
[24]. Jusas, V., & Samuvel, S. G. (2019). Classification of motor imagery using combination of feature extraction and reduction methods for brain-computer interface. Information Technology and Control, 48(2), 225–234. https://doi.org/10.5755/j01.itc.48.2.23091