ENHANCED COMPUTATION ARCHITECTURE FOR BIG DATA ANALYTICS USING ENCRYPTION ALGORITHM

Praveen Banasode
Assistant Professor
Department of Master of Computer Applications,
Jain College of Engineering, Belagavi Karnataka, India
praveenb.jce@gmail.com

Sunita Padmannavar
Assistant Professor
Department of Master of Computer Applications
Gogte Institute of Technology, Belagavi, Karnataka State, India
sunitapdm@gmail.com

Abstract

Big data infrastructure needs to be structured in the most critical aspects and wisely calculate how large data applications are managed in order to achieve the most important security issues required. One of them is privacy is a related feature as users can share more and more personal data and content and public clouds on social networks through their devices and computers. The previous system have some drawbacks, it is not secure the sensitive data storage security of privacy issues in the big data. However, the existing encryption system for data cannot protect the access mode, and it can also leak sensitive information. To overcome the issues in this work proposed the method Transparent Secure Hashing Data Optimized Privacy Protection Encryption (TSHDOPPE) Algorithm for Encryption of data can prevent permission to use the unwanted users' associated data storage system of data. Less storage leakage overhead and efficiency are proposed. It includes stored in a transparent data protected for data at rest and could not leak the Data for data in Transit. Non-relational data storage and protection data storage has been a TSHDOPPE algorithm used to ensure the transaction log. In the data used for stored in cloud computing, managing user data optimizing the Improved Deep Neural Network (IDNN) is reduces difficult and reduces the cost of maintaining data. Unprotected data in Transit or at rest, or vulnerable to attacks, companies are also effective security measures that provide protected data with strong data protection between the device and the network in these conditions.

Keywords*: Big data, Data Management; Transparent Secure Hashing Data Optimized Privacy Protection Encryption (TSHDOPPE); Data Protection; Improved Deep Neural Network (IDNN); Data Rest and Transit; encryption.*

1. Introduction

Big data processing, data is stored in a large area can store, data extraction and processing a large number of cloud environment of large amounts of data, but there will be security problems. In such a virtual machine behavior of large enterprises and enterprise data, a machine has access to all the data required in another machine. Cloud computing is a computing model, the application is connected to a private or public network provided data and file storage dynamically scalable infrastructure system. For example, things, keep track of rising targeted advertising and location of the smartphone, and increase Internet use of the collected personal statistics, all of the new analysis and services, represent a new opportunity for the health and wellness equipment. The collected Data, in many cases, have been included in the fall in the wrong hands would bring great harm, personal information about individuals and companies secrets. Crime groups, it is possible to buy and sell the personal information people are stolen, have to create an underground market. Intelligence agencies of the government, private for all competitive advantage, companies, and government enemy spy and systems

have been the target. If this potential harm these organizations can cost millions of dollars, causing serious damage to individuals and institutions affected, commercial, recently many of the government targets, is evidenced.

To clarify these examples, new and enhanced security tools allow applications to enjoy big data analytics benefits without the risk of such catastrophic attacks, collect and big. Need to protect the system for processing data of modern cryptography provides many powerful technologies that can protect the entire data lifecycle of big data applications because it is stored in the warehouse where it is collected and processed through analysis. Big Data is considered a paradigm for the next generation of computing. Many industries have recently moved to big data, so they tend to store data in it, including a cloud of network-denial data. Data security and storage security has always been a major issue of information technology. Data is located in a different location because it spread worldwide; in the big data environment, it becomes particularly acute. The cloud service provider is responsible for providing this data security. Besides, cloud users, because they just protect their data, it is impossible to rely on the service provider; there is a responsibility to protect their data.

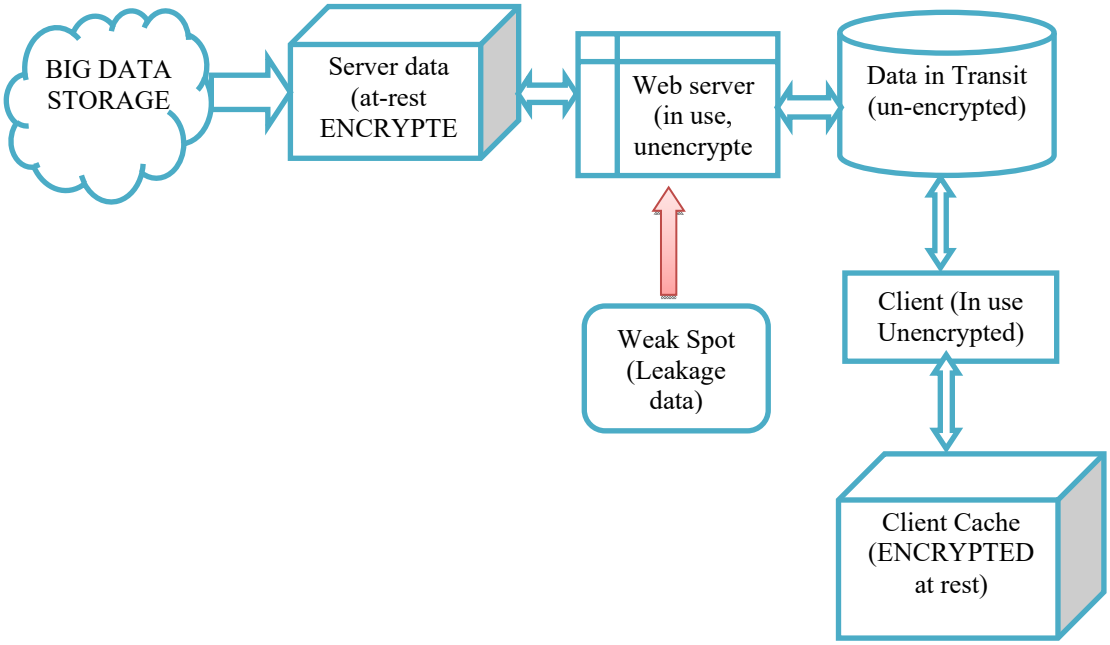

Figure 1: Big data computing analytics architecture for Data Rest and Data Transit.

Figure 1 describes big data structures refer to logical and physical structure, are used to indicate large amounts of data ingestion, process, stored, managed and accessed. It used to manage large data's and it can analysis tool for business purposes, steer data analytics, and it is possible to provide environment which it is used to big data analytics to extract business information from other critical data.

The architecture contains four layers:

- ***Big Data Sources Layer*:** In the big data environment, it can be manage both batch processing and real-time processing of big data sources, such as data warehouse, relational database management system, SaaS applications, and internet of things.
- ***Management & Storage Layer*:** it receiving data from a source and it converts the data into a format for data analysis tool and store data to its relevant format.
- ***Analysis Layer*:** Analysis tools, extract the business intelligence from big data storage layer.
- ***Consumption Layer*:** Receiving a result from the big data analysis layer, and it presents to an output layer it also known as business intelligence layer.

To protect the data at rest, it will be based on the security; there can, in many cases, be lose in security. Data for storage device, using a protocol such as regarded as static, moves over the network. It sounds a little illogical, but there is a possibility that the move also media data that is stored. For example, ships a large number of backup tapes containing sensitive data might carry in a pocket, including a tax form on the car's back seat. The content of the customer database, laptop copy or fake flash drive, Deduplication of encrypted Data is a promising trend for two cloud storage providers and users. Data deduplication allows Cloud Service Providers (CSPs) to save storage space by eliminating copies of the same data. Data encryption can ensure customer

confidentiality for both resting traffic and data. However, the data deduplication feature works when it can't work well with traditional encryption to detect the same data and provide encrypted data. Encryption of the same data using different keys (by different users) will result in different cipher texts, but the CSP cannot perform data deduplication. It is deployed on the premises of the cloud service provider called Deduplication and forwards holomorphic encryption, with the key Server's help, a plan to allow the encryption and Deduplication, and place. In this solution, the user, using the encryption key data of the encrypted data, uses the encryption key from the Server through a variety of key management schemes.

2. Related Work

Big data Security provide identity-based broadcast Encryption for polynomial interpolation theorems for re-encrypted using cipher text receipts commercial broadcasters to provide identity of the data users [1]. Re-encryption proxy is a valid solution to securely share the cloud data and the receiver. Groups of receivers, the shared Data, and the sender must re-generate the re-encryption key for each receiver overhead to the transmission side [2]. Cloud service providers that use Hadoop software, providing the popular Hadoop analytics platform with service follow-up, the computing infrastructure has been positive to have clusters of machines in their cloud [3]. Local use of these products can complicate the local use of cost and similar systems, but reduce security considerations, and companies, especially through the data protection basket, can use this service emotionally and qualitatively process data. Adaptation and secure Identity-based broadcast encryption systems are, in the standard model, equipped with a certain size cipher text [4]. The secret key of the size of the public key is linear to the maximum number of recipients [5]. Also, our system is completely rigging, has a stateless receiver. Compared to the cutting-edge, program is good, and it has been optimized for broadcast encryption [6]. As growing numbers alarming rate of cloud services, more and more service providers provide a similar function [7].

User non-functional attributes required for the service that has been selected, very important, have caused some of the big data-related challenges for the search ranking of cloud data that has been encrypted, save Order Preserving Encryption (OPE) is a valid tool for inverting the index's encryption relevance score [8] [9]. To use a deterministic OPE is the distribution of the correlation score that is revealed in the cipher text. Probability OPE called one-to-many of OPE can be combined with the distribution of the plaintext [10] [11]. Tools and Privacy: basic expectations for applications using a cloud of confidential and personal data. [12]. There are some general approaches to this problem. To do this is to make information theft incidents very difficult. Although customers usually have to believe that these policies are actually in use, they are effective infrastructure management principles working through cloud service providers. The solution provided by the database system supplier is encrypted data, which unfortunately provides a very limited purpose for solving privacy and security issues. Due to the complexity of cloud computing's ecosystem, there is a growing concern about the usefulness of the Privacy of the cost and data. State-of-the-art encryption methods, but to protect the user's Privacy, exclude the meaningful calculation in the encrypted data [13]. Searchable Encryption (SE) such as encrypted search technology, because it is designed for use in data types of the same type, such as text or digital, a plurality of technologies to a Database Management System (DBMS) 14]. Such an assumption is, has led to such a heterogeneous effort integration script, popular design, such as network Internet through the techniques of things, accelerate the generation and collection of big data unprecedented scale, and provides an integrated infrastructure and smart application [15]. However, as our basic products in the current information age, big Data is the key to an important competitive edge in modern business.

Privacy Deep Neural Network (DNN) system saved not only us, to apply the image DNNs without visual information, as well as, but the use of separate encryption key for the first time of training and test image can also consider it [16]. With the new development of cloud computing, the cloud has become a trend of aggregation of big data used to store outsourcing and large quantities of information. Participated in the rich value of big data, the machine learning method has been using the ability to adapt to changes in the Data because it is in general. Since they are unwilling to share their information, however, the data mining process can include the user's privacy issues. Big data, such as a user's interaction in the joint filter's customer evaluation matrix with such social network, has an important value for companies and research. As it is large-scale, they are not only always maintaining, and require a lot of computing resources [17]. With a wide range of deployment of public cloud resources, the owner, to obtain storage and computing scalability, is recommended to use the cloud resources. However, the privacy and cloud map has been attracting attention.

3. Methodology

A big Data application usually refers to run on large data sets large-scale distributed applications. Data exploration and analysis has become a major problem in many time span of big data. Large and complex data are difficult to process with traditional data processing applications, the development of its calculation triggered large data applications. However, it is a remarkable contradiction between the widespread use of Privacy and

big data security and big data. The data collected from structured and unstructured data sources. This hierarchical and transformation and data integration, and stream computing machine are stored in different data repositories. A different approach is Transparent Secure Hashing Data Optimized Privacy Protection Encryption (TSHDOPPE), which takes into account the specific risks of the cloud, expands encryption to hide the data in use and a portion of the data in operation, and can perform a large subset of Structured Query Language (SQL), including heavy-data related functions, functions and transactions. Using Transparent Secure Hashing Data Optimized Privacy Protection Encryption (TSHDOPPE) for TransCrypt conceptualization, design and implementation, Which uses a high level of advanced key management scheme for encrypted file system to provide security while remaining transparent and easy to use. Improved Deep Neural Network (IDNN) is considered difficult issues optimized, such as the super-user account or a trust to avoid privileged user process space, and presented their new solution. These enhancements make TransCrypt, in order to prevent a broader threat model and solve the existing system in a number data rest and transit.

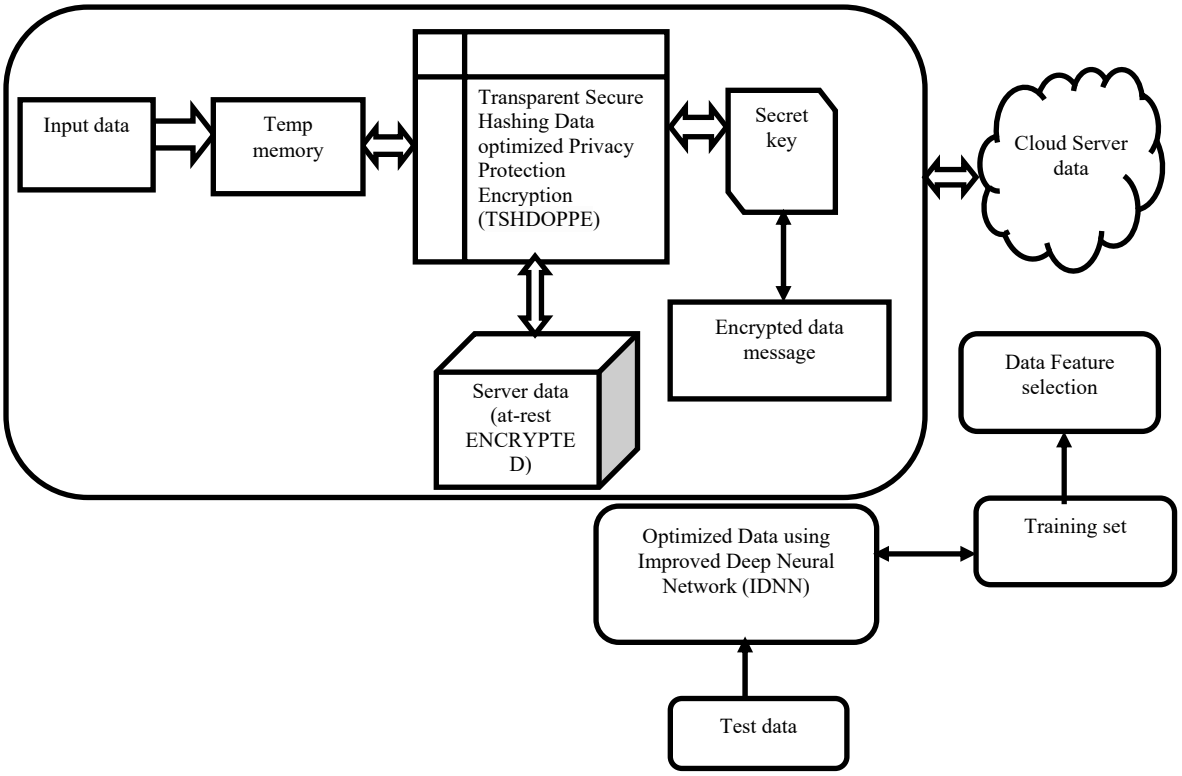

Figure 2: Proposed system for Data Rest and Data Transit.

Figure 2 describes the Web server processes the incoming request and it is recommended that transparently decrypt the requested data. In the proposed method TSHDOPPE manages duplication removing process using the encrypted data. The appropriate leakage data may be able to instant access to Data that is not encrypted. In the optimization using Deep Neural Network (DNN) analysis the feature selection based on the training dataset stored in the cloud data server.

3.1 Secure Encryption Method at Data Rest

Static data refers to the analysis of the collected information from various channels and generated created events. From the analysis's conclusions, it will take by the data analysis are divided clearly. Since the encryption key's concealment is applied to security and concealment, it is safe to encrypt sensitive data in the database. The encryption key is unknown to anyone but does not exist on all the systems. Secure than other methods of securing the key that is used to modify more data. For static data, the batch processing method has been commonly used. In this case, although there is no urgent need for infrastructure always-on, very large, in many cases, there is flexibility required to support a non-structured data set. From the viewpoint of cost, the public cloud can be ideally selected. In this case, the infrastructure needs to analyze the data.

Steps for Encrypting Data at Rest

```
Step 1: Data at Rest (Static)
      Inactive And Not-changing data
Step 2: Encrypt Elements ←[], Encrypt Formats ←[], H-0;
                If (each Elements. Get Values () = null)
                        If Each Element. Get Values ();
                        Each Formats [H]←Each Elements;
                Else
                        Encrypt Elements [H] ← each elements
                        Each Format [H]
                        Each Elements .get Values ("data. Encrypt")
                   End if
Step 3: Data at Rest (inconsistent)
      Referencing the Inactive data to change
Step 4: Data in use
```

Where, H- Variables declaration, some of the Data elements is static and data transit it is possible to encrypt data can be read. The data collection process in the mobile is the same as the resting of data, the analysis. However, the difference lies. In this case, real-time analysis is due to the occurrence of an event.

3.2 Secure Encryption method using Data Transmission

Data security in Transit refers to the transmission of data security in the cloud. Data in Transit to be very sensitive, such as user name and password to move from one place to another, data on the road might be more dangerous than the break data. Its purpose is to highlight the major issues related to data security in the cloud environment. Large data processing architecture is sent from the user, or other sources collected in a central repository, as it is stored in the data can be analyzed. Data must ensure that all the data in a protected manner transfer to ensure that it failed to reach the destination and unstable. It is in the prior art and tools Internet Protocol security provided by lifecycle stage, and Transport Layer Security for a big data tools standardization and dissemination of concern. These issues were divided into three categories: Compared to the traditional infrastructure data security issues raised by a single cloud property, up data security data lifecycle calculated data storage, transfer and use of the cloud, attribute data security and data security confidentiality, integrity and availability. Each category is emphasized in the general cloud computing solutions for data security. Database log files from the big event of data from multiple sources data intrusion prevention system security controls such as data information. Data security is essential for any organization, must be an encryption key. The problem for the owner is to maintain control of his data to another creation. For personal information and personal information, car owners must know the personal information is collected to use.

3.3 Optimization using Improved Deep Neural Network (IDNN) in big data

The probability of failure in each category is high, and our recovery mechanism has low performance due to fierce competition with the data system and failure unit. However, when use more partitions, need more bits per block. These tracks overlap for greater metadata storage. However, these individual partitions are more likely to deal with failures. Optimized Improved Deep Neural Network (IDNN) for computing Big Data problem, lots of work has been carried out. As a result various types of technologies have been developed. As the world is getting digitized the speed in which the amount of data is over owing from different sources in different format, it is not possible for the traditional system to compute and analysis this kind of big data for which big data tool is used which is an open source software. Recent optimization technologies and their applications developed for Big Data. To help, choose the right collaboration of various Big Data technologies according to requirements.

3.4 Hashing Privacy Protection Secure Encryption Using Data Rest and Transit

Big data applications please refer to its normal work in large-scale distributed applications with large data sets. Analysis and data search in the range of big data has become a troublesome problem in many sectors. With the continuous increase of large-scale multi-source heterogeneous big data, high requirements for speed of data analysis have increased. Use the Transparent Secure Hashing Data Optimized Privacy Protection Encryption (TSHDOPPE) algorithm for encryption and decryption of data, with the help to avoid the problem and secure data protection of big data, to change the concept of a hash value recommend. TSHDOPPE algorithm less time-consuming than shown earlier hash techniques for the results to compare the security and time consuming based on proposed the system. Optimization the design to take full advantage of the available resources as specified

by the application optimization to make full use of the large amount of space or speed available in memory on a particular computer. Optimization is to compare a set of selection controls including factors such as efficiency, productivity, reliability, life, maximum degree of strength, and use the best strategy to achieve.

Algorithm steps for TSHDOPPE

Input: Data Retrieved for the Server
Output: Data Information Decrypted using

Step 1: Begin
Step 2: In the data from the database, sensitive data only read
Sender Plaintext Information (Using Secure Hashing algorithm)
Step 3: In the Server-side data at Rest
Step 4: In the Server, information is used to decrypt for the client
Step 5: Data at Transit is encrypted
Step 6: TSHDOPPE →using Transparent optimized Secure Hash Key for decrypting the data in the Server to client
Step 7: Generating the secret Key for encryption of data message
Step 8**:** Store in data set big data storage.
Step 9: Encryption of the basic data.
TSHDOPPE algorithm of applications clouded the big data to implement the encryption.
The private key decrypts the public key to encrypt the data.
Step 10: Information that is guaranteed by the hash structure is stored on the Server.
Step 11: Stop

Where, TSHDOPPE - Transparent Secure Hashing Data Optimized Privacy Protection Encryption, Data is protected information stored in the big data is received from the Server, because there is an information data of the database. It is divided the original of data in the vertical and horizontal directions to learn to use a hash function. Decrypting of information from the server is processed by the transparent algorithm.

4. Experimental Evaluation

The hash function provides an improved size and performance to produce results on the improved security. First of all, it is a basic modern security model. Also, it is used to convert a substantial amount of random information into small, fixed data. Also, the Algorithm is used (at rest and transit data). However, because it does not depend on the primary or secondary key for the system to operate, the encoding improves a one-way operation. To maintain and allows their security mechanism using Algorithm and verification, compares the previous and the proposed method.

No. of. data	OPE in %	SE in %	TSHDOPPE in %
200	30	35	39
400	37	40	44
600	41	45	50
800	47	54	61
1000	58	68	81

Table 1: Analysis of the Security Level.

Table 1 describes the security level for privacy protection, improving the results for comparing the existing and proposed methods.

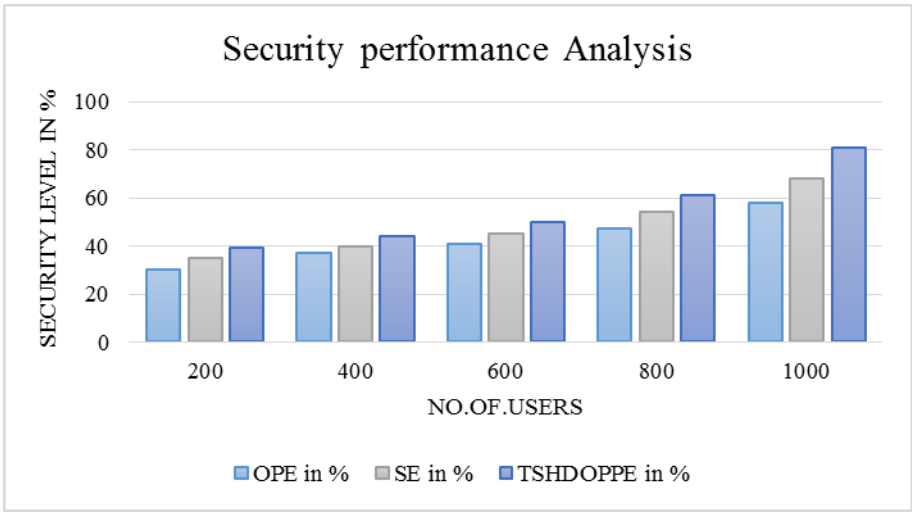

Figure 3: Analysis of the Security Performance.

Figure 3 describes the security performance improving the Data at rest and Transit time. The proposed Algorithm improved the security performance compared to the existing method. In the proposed method Transparent Secure Hashing Data Optimized Privacy Protection Encryption (TSHDOPPE) algorithm is 81% better than previous methods.

No. of. data	OPE in sec	SE in sec	TSHDOPPE in sec
200	34	29	25
400	40	37	35
600	46	43	39
800	51	49	47
1000	59	55	52

Table 2: Analysis of Transmission Delay.

Table 2 shows the Data transmission delay performance based on the exiting and previous algorithms; improving the Data transfers is taking a Low time using the Transparent Secure Hashing Data Optimized Privacy Protection Encryption (TSHDOPPE) algorithm.

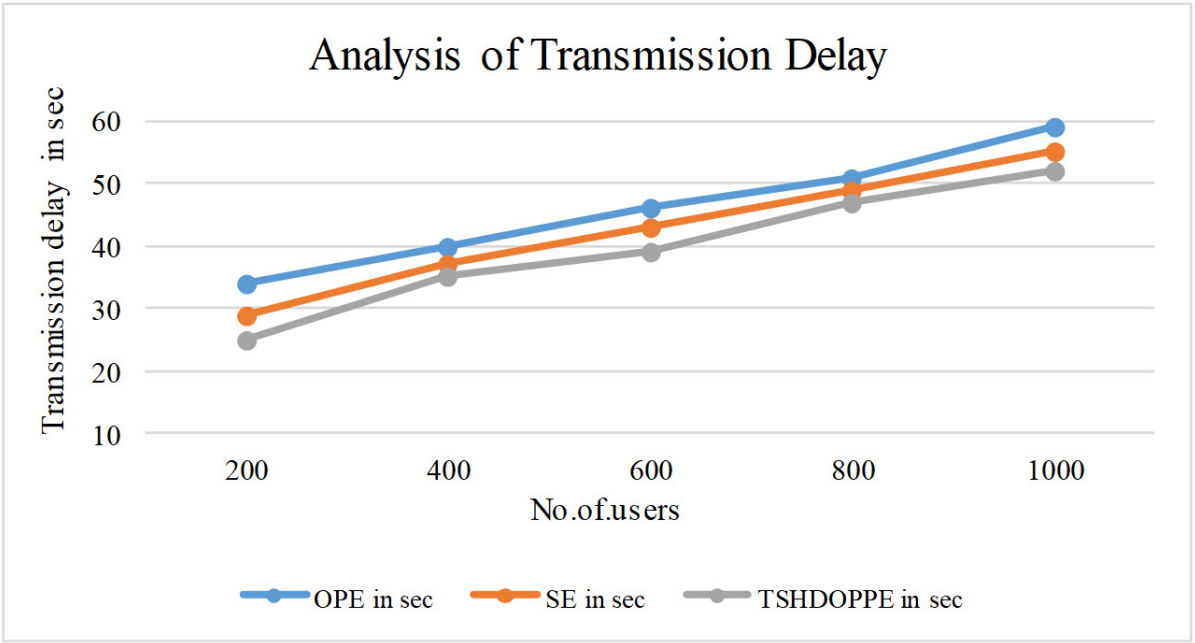

Figure 4: Analysis of Transmission delay.

Figure 4 describes the data transfer rate based on the existing and proposed methods. In the proposed method is reduces the Transmission delay in 52 sec during the data transmission for 1000 data.

Num.of.Data	OPE in %	SE in %	TSHDOPPE in %
200	37	34	29
400	41	37	33
600	47	41	36
800	51	45	40
1000	60	59	55

Table 3: Data storage Space Optimization

Table 3 shows the Optimized data storage in the big data based on the encryption algorithms, in the comparison of methods are using the data rest and transit from big data computing architecture.

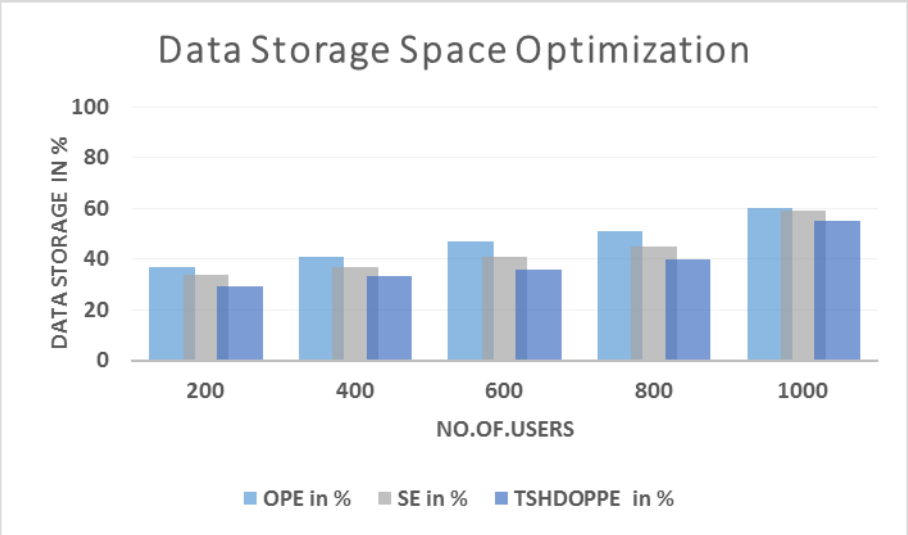

Figure 5: Data Storage Space Optimization

Figure 5 describes the detecting the data storage improves based on the existing and proposed comparisons, in the proposed Transparent Secure Hashing Data Optimized Privacy Protection Encryption (TSHDOPPE) algorithm is addressing 55% of comprising the data storage space for 1000 data in big data optimizing.

Num.of.Data	OPE in sec	SE in sec	TSHDOPPE in sec
200	39	35	30
400	46	40	38
600	50	47	44
800	55	51	48
1000	57	54	50

Table 4: Encryption Time Analysis

Table 4 shows the encryption time based on the previous and proposed system comparisons; in the Encrypting the data within the minimum time taken for proposed method.

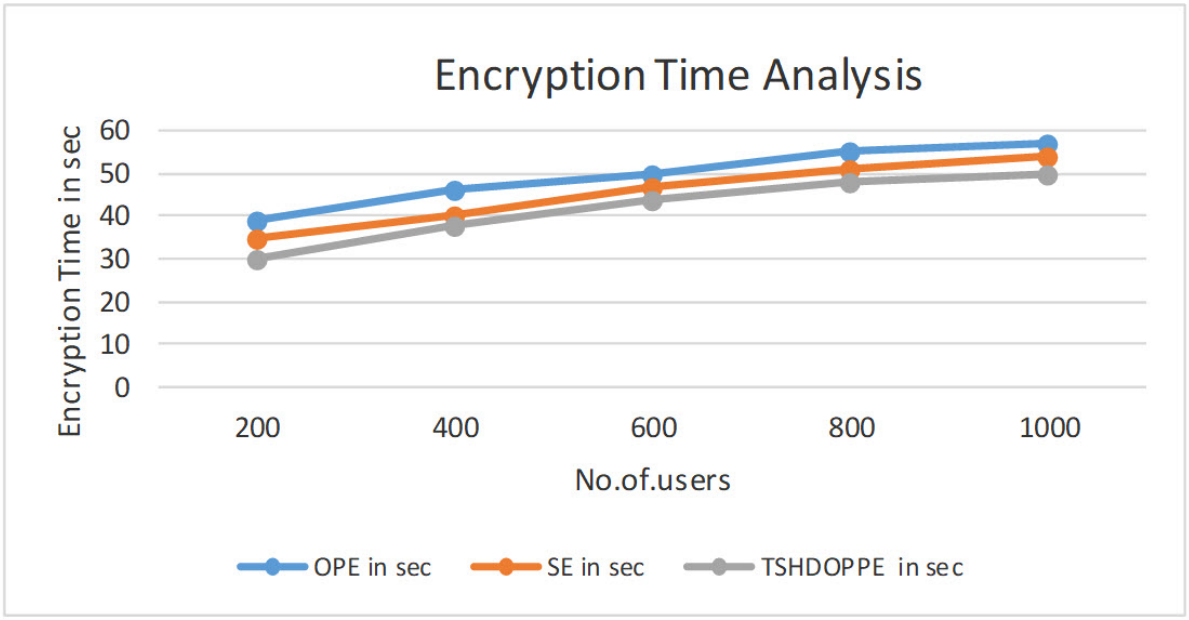

Figure 6: Encryption Time Analysis

Figure 6 shows the encryption time for a data security in big data analytics, in the proposed system Transparent Secure Hashing Data Optimized Privacy Protection Encryption (TSHDOPPE) algorithm take a 50 sec for encryption better the previous methods.

No. of. data	OPE in %	SE in %	TSHDOPPE in %
200	31	25	22
400	40	35	30
600	46	43	35
800	50	47	43
1000	55	52	51

Table 5: Optimized Error Rate Analysis

Table 5 describes the Error rate based the time limitation, compares the previous and proposed system. In the time limitations, are data at rest, and data transfers are analyzed in minimum time.

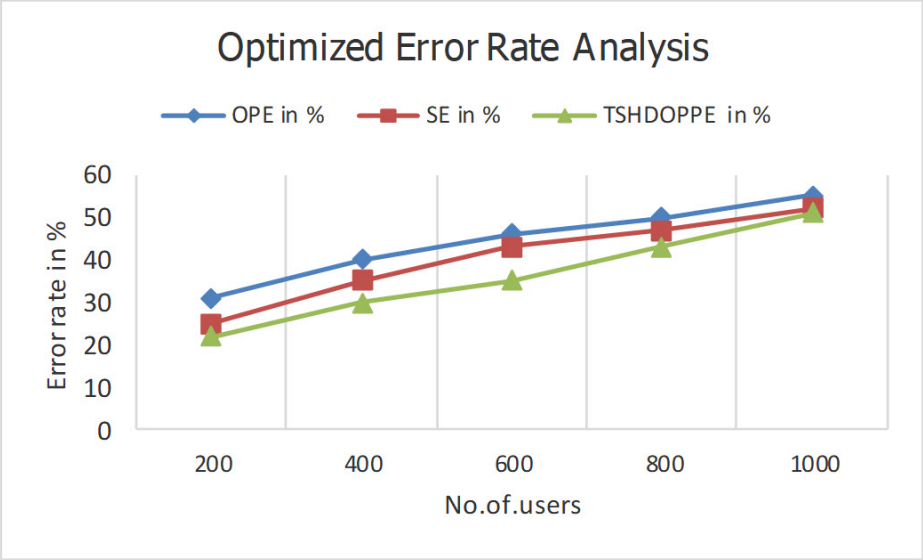

Figure 8: Optimized Error Rate Analysis

Figure 8 describes the Error rate analysis the comparison of previous and proposed methods. In the data transfers are in Server within minimum time, the proposed method, Transparent Secure Hashing Data Optimized Privacy Protection Encryption (TSHDOPPE) algorithm, is 51 % of data transfer and data rest.

5. Conclusion

Big Data platform provides data platform products and data services and business units using the intrinsic value of the data through the integration of all data and comprehensive analysis. Since most Transparent Secure Hashing Data Optimized Privacy Protection Encryption (TSHDOPPE) algorithms support the security level of the movement and storage of data, since these algorithms, it can occur in many examples of security problems from time to time. In the proposed method, TSHDOPPE has analyzed the security level is 81%. The Transmission delay is reduced within 52sec, Data storage space optimized in 55% comprising the data for storage, Encryption time reduced 50sec in and Error rate is 51 % for 1000 data; there may be some of the most important security and privacy issues optimized using Improved Deep Neural Network (IDNN) specificity of big data. In the proposed method reduced the leakages and improving the security based on the minimum time. Security to ensure of the big data characteristics also proposes solutions to these problems, but it does not provide a final solution to this problem. And it points out some directions and technologies that may help solve some of the most relevant and challenging big data security and privacy.

References

[1] S. Maiti and S. Misra, "P2B: Privacy-Preserving Identity-Based Broadcast Proxy Re-Encryption," in IEEE Transactions on Vehicular Technology, vol. 69, no. 5, pp. 5610-5617, May 2020, doi: 10.1109/TVT.2020.2982422.
[2] A. C. Mert, E. Öztürk and E. Savaş, "Design and Implementation of Encryption/Decryption Architectures for BFV Homomorphic Encryption Scheme," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 28, no. 2, pp. 353-362, Feb. 2020, doi: 10.1109/TVLSI.2019.2943127.
[3] H. Wang, C. Yu, L. Wang and Q. Yu, "Effective BigData-Space Service Selection over Trust and Heterogeneous QoS Preferences," in IEEE Transactions on Services Computing, vol. 11, no. 4, pp. 644-657, 1 July-Aug. 2018, doi: 10.1109/TSC.2015.2480393.
[4] H. Wang, X. Dong and Z. Cao, "Multi-Value-Independent Ciphertext-Policy Attribute-Based Encryption with Fast Keyword Search," IEEE Transactions on Services Computing, vol. 13, no. 6, pp. 1142-1151, 1 Nov.-Dec. 2020, doi: 10.1109/TSC.2017.2753231.
[5] S. Ramesh and M. Govindarasu, "An Efficient Framework for Privacy-Preserving Computations on Encrypted IoT Data," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8700-8708, Sept. 2020, doi: 10.1109/JIOT.2020.2998109.
[6] S. Chung, M. Shieh, T. Chiueh, C. Liu and C. Tu, "uFETCH: A Unified Searchable Encryption Scheme and Its Saas-Native to Make DBMS Privacy-Preserving," in IEEE Access, vol. 8, pp. 93894-93906, 2020, doi: 10.1109/ACCESS.2020.2994598.
[7] W. Gao, W. Yu, F. Liang, W. G. Hatcher and C. Lu, "Privacy-Preserving Auction for Big Data Trading Using Homomorphic Encryption," in IEEE Transactions on Network Science and Engineering, vol. 7, no. 2, pp. 776-791, 1 April-June 2020, doi: 10.1109/TNSE.2018.2846736.
[8] Y. Li, G. Liu, Z. Zhang, J. Luo and F. Zhang, "CityLine: Designing Hybrid Hub-and-Spoke Transit System with Urban Big Data," in IEEE Transactions on Big Data, vol. 5, no. 4, pp. 576-587, 1 Dec. 2019, doi: 10.1109/TBDATA.2018.2840222.
[9] K. Guntupally, R. Devarakonda and K. Kehoe, "Spring Boot based REST API to Improve Data Quality Report Generation for Big Scientific Data: ARM Data Center Example," 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 5328-5329, doi: 10.1109/BigData.2018.8621924.
[10] H. Ferguson, C. Vardeman and J. Nabrzyski, "Linked data platform for building cloud-based smart applications and connecting API access points with data discovery techniques," 2016 IEEE International Conference on Big Data (Big Data), Washington, DC, USA, 2016, pp. 3016-3025, doi: 10.1109/BigData.2016.7840955.
[11] S. Sen and C. Jayawardena, "Operational Performance and Security Improvement Approach for Integrated BigData and Industrial IoT in Cyber-Physical Communication Systems," 2019 International Conference on High Performance Big Data and Intelligent Systems (HPBD&IS), Shenzhen, China, 2019, pp. 47-54, doi: 10.1109/HPBDIS.2019.8735468.
[12] W. Sirichotedumrong, Y. Kinoshita and H. Kiya, "Pixel-Based Image Encryption Without Key Management for Privacy-Preserving Deep Neural Networks," IEEE Access, vol. 7, pp. 177844-177855, 2019, doi: 10.1109/ACCESS.2019.2959017.
[13] X. Dong, J. Chen, K. Zhang and H. Qian, "Privacy-Preserving Locally Weighted Linear Regression Over Encrypted Millions of Data," in IEEE Access, vol. 8, pp. 2247-2257, 2020, doi: 10.1109/ACCESS.2019.2962700.
[14] S. Sharma, J. Powers and K. Chen, "PrivateGraph: Privacy-Preserving Spectral Analysis of Encrypted Graphs in the Cloud," in IEEE Transactions on Knowledge and Data Engineering, vol. 31, no. 5, pp. 981-995, 1 May 2019, doi: 10.1109/TKDE.2018.2847662.
[15] Y. Sun, X. Li, F. Lv and B. Hu, "Research on Logistics Information Blockchain Data Query Algorithm Based on Searchable Encryption," in IEEE Access, vol. 9, pp. 20968-20976, 2021, doi: 10.1109/ACCESS.2021.3054557.
[16] S. Yao, R. V. J. Dayot, H. -J. Kim and I. -H. Ra, "A Novel Revocable and Identity-Based Conditional Proxy Re-Encryption Scheme With Ciphertext Evolution for Secure Cloud Data Sharing," in IEEE Access, vol. 9, pp. 42801-42816, 2021, doi: 10.1109/ACCESS.2021.3064863.
[17] W. Feng, Y. He, H. Li and C. Li, "A Plain-Image-Related Chaotic Image Encryption Algorithm Based on DNA Sequence Operation and Discrete Logarithm," in IEEE Access, vol. 7, pp. 181589-181609, 2019, doi: 10.1109/ACCESS.2019.2959137.

Authors Profile

Praveen Banasode is an Assistant Professor at Jain College of Engineering ,Belagavi Karnataka State, India Where he received his Bachelor degree in Computer Science in 2005. He received his Master Degree from Gogte Institute of Technology in Computers in 2008 from Visvesvaraya Technological University, Belagavi Karnatak India. He has published several articles on Big Data analytics. He has supervised groups of postgraduate projects in various aspects of computer applications.

Dr. Sunita S. Padmannavar: Working as a Assistant Professor, M.C.A. Department, KLS's Gogte Institute of Technology, Belagavi, Karnataka, India. She has 14 years teaching and 13 years research experience. She published 02 papers in national journals, 21 papers in international journals and 05 papers in conferences. Also she is author of 2 books. Her research area includes Web technology, IOT, Big data and Cloud computing. **L**ife time member of International Society for Research and Development (**ISRD**). Award of the highest order - Dr. Sarvepalli Radhakrishnan Award - for contribution towards nation's development from Mentrox on 5th September 2020. Won Best Paper Award in International Conference GIT-2010 "Green-It & Open Source" organized by Sinhgad Institute of Management, Pune in association with University of Pune & Computer Society of India (CSI) on 20-22 Feb 2010.