Secure Cloud Data in Decomposition of Encrypted Tensor using Homomorphic Encryption Scheme

Sinduja T[1]
Student,Dept. of CS&E,
VTU Regional Centre, Mysuru,
India

Dr. K. Thippeswamy[2]
Professor and Head,
Dept. of CS &E,VTU Regional Centre,
Mysuru, India

***Abstract*:- As the quickly developing volume of information are past the capacities of numerous figuring frameworks, to safely handle them on cloud has turned into a favored arrangement which can both use the effective abilities gave by cloud and ensure information protection. This paper shows a way to deal with safely deteriorate a tensor, a scientific model generally utilized as a part of information serious applications, to a center tensor duplicated with a specific number of truncated orthogonal bases. The unstructured, semi-organized, and organized information are spoken to as low-request sub-tensors which are then scrambled utilizing the completely homomorphic encryption plan. A brought together high-arrange figure tensor model is developed by gathering all the figure sub-tensors and installing them to a base tensor space. The figure tensor is disintegrated through a proposed secure calculation, in which the square root operations are wiped out amid the Lanczos strategy. Hypothetical examinations of the calculation as far as time many-sided quality, memory utilization, disintegration exactness, and information security are given. Test results show that the methodology can safely decay a tensor.With the headway of completely homomorphic encryption plan, it can be normal that the safe tensor disintegration approach can possibly be connected on cloud for security saving information preparing.**

Record Terms — Tensor Decomposition, Fully Homomorphic Encryption, Lanczos Method, Cloud.

1. PRESENTATION

The measure of information in numerous fields is quickly expanding towards Terabyte level or even Petabyte level, and in addition the information structures are turning out to be more changed. The substantial scale heterogeneous information have postured extraordinary difficulties on current figuring bases, and new methodologies are in dire need to address them. Distributed computing is a model that can empower pervasive and helpful system access to a common pool of configurable figuring assets, for example, stages, programming and administrations. A cloud framework is the gathering of equipment and programming which can give abilities to the shoppers on a compensation for every utilization or charge per-use premise. It is an entirely possible way to deal with transfer the substantial scale information to cloud for profoundly handling and mining, for example, dimensionality decrease , characterization , and forecast . In any case, doing such sorts of errands on cloud may bring about a progression of security issues including loss of protection, divulgence of business data, information alter, and so on. Thusly, the investigation of secure information mining and information examining on cloud is of awesome need as it is an effective strategy to concentrate significant data from the vast scale heterogeneous information. The completely homomorphic encryption plan, which is proposed in 1978 by Rivest, Adleman, Dertouzos , permits particular sorts of calculations to be performed on the cyphertext to produce a scrambled result, of which the unscrambling is indistinguishable to the outcome got by straightforwardly doing operations on the plaintext. The perfect cross section based plan proposed by Gentry in 2009 takes care of the issue of set number of operations of completely homomorphic encryption, which makes ready for trusted figuring on cloud. The Learning with Errors (LWE) plan reported in is more functional to be utilized in information concentrated applications. In spite of the fact that the specified plans give both added substance and multiplicative homomorphisms, they can bring about unscrambling blunders when be utilized by calculations including non-homomorphic operations, for example, square root and division, which are every now and again utilized operations amid information preparing. Numerous heterogenous information are displayed as tensors [8, 9], a kind of high measurement lattice broadly utilized as a part of numerous applications. Tensor deterioration is a capable apparatus to concentrate significant data from expansive scale crude information. The disintegration is computationally costly and is unequivocally proposed to be performed on cloud. Along these lines, it is important to explore approaches for secure tensor decay on cloud and address the difficulties brought about by non-homomorphic operations. Be that as it may, little research has been given to such kind of technique. This paper introduces another registering approach which can safely break down the tensor model created from expansive scale heterogeneous information.

The significant commitments are compressed as takes after.

• We exhibit an all encompassing structure to address the issue of secure tensor deterioration on cloud. The structure not just permits us to use the intense computational capacities of the cloud, additionally guarantees information security amid the procedure of tensor decay.

- We present a Unified Cipher Tensor (UCT) model for heterogeneous information representation. The itemized methodology of how to encode the low-arrange sub-tensors developed from heterogeneous dat as figure partners utilizing the completely encryption plan, and how to implant them to a base tensor space to produce a brought together figure tensor model are outlined in this paper.

- We propose to utilize the Lanczos technique to deteriorate the produced figure tensor model to a center tensor and a specific number of truncated orthogonal bases. A protected tensor decay calculation is outlined in which the nonhomomorphic square root operations are evacuated amid the Lanczos technique.Hypothetical examinations of the calculation as far as time multifaceted nature, memory utilization, disintegration exactness, and information security are given.

2 PRELIMINARIES

In this area, the preliminaries on tensor decomposition,fully homomorphic encryption, and Lanczos method are audited.

2.1 Tensor Decomposition

Tensor is a kind of high measurement framework broadly utilized as a part of numerous applications, for example, PC vision, information mining, chart examination and sign preparing. High-Order Singular Value Decomposition (HO-SVD) is a kind of methodology that can factorize the tensor to a center tensor duplicated with various truncated orthogonal lattices. Let T ∈ RI1×I2×:::×IN mean a N-th request tensor model, S and ^ T allude to the center tensor and rough tensor individually, then the HO-SVD strategy is characterized as

$$S = T\times_1 U_1{}^T \times_2 U_2{}^T \ldots \times_N U_N{}^T,$$
$$\hat{T} = S\times{}_1U_1 \times_2 U_2 \ldots \times{}_N U_N \qquad (1)$$

The i-mode item T×iU; 1 ≤ i ≤ N, of a tensor by a lattice in Eq. (1) is characterized as

$$(T\times_i U)_{j_1 j_2\ldots j_{i-1} k_i j_{i+1}\ldots j_N} = \sum_{j_i=1}^{I_i} (t_{j_1 j_2 \ldots j_{i-1} j_i j_{i+1} \ldots j_N} \times u_{k_i j_i}), \qquad (2)$$

where tj1j2… ji-1jiji+1… ji and ukiji allude to the components of tensor T and lattice U, respectively.

TABLE 1
Table of symbols.

Symbol	Definition
T	initial tensor
S	core tensor
$\hat{T}$	approximate tensor
$T_{(i)}$	i-mode unfolded matrix
$Sym(T_{(i)})$	symmetric matrix generated with $T_{(i)}$
D_u, D_{semi}, D_s	unstructured, semi-structured, structured data
L	tridiagonal matrix
α, β	elements of the tridiagonal matrix
U (V)	left (right) singular vector matrix
Σ (Λ)	singular (eigen) value
$\times_i$	i-mode product of a tensor by a matrix
$\mathcal{R}$	set of real numbers
$\mathcal{Z}$	set of integers
R ($R[x]$)	ring (polynomial ring)
m	plaintext
c	ciphertext
χ	discrete gauss distribution
e	randomly selected error from χ
q, p	big prime integers
Enc (Dec)	encryption (decryption) function
Ψ^E	cipher data of Ψ, namely $\Psi^E = Enc(\Psi)$

For instance, Fig. 1 exhibits the created center tensor S and the truncated bases U1, U2, U3 by breaking down the underlying tensor T. The 4 by 4 by 3 tensor is decayed to a 2 by 2 by 2 center tensor, two frameworks of 4 by 2 and a network of 3 by 2. By and large, the center tensor and the truncated bases are considered as a compacted rendition of the underlying tensor T. The remade information in the surmised Tensor Tˆ are of higher quality than the crude information as the commotion, inessential and conflicting information are expelled.

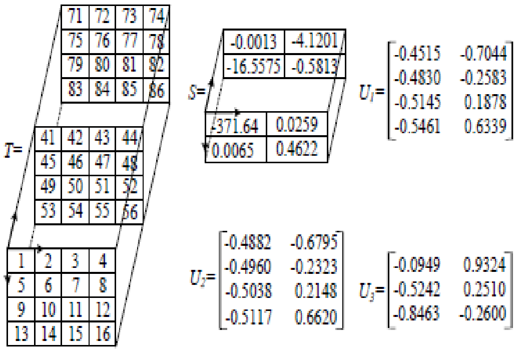


Fig. 1. Decomposing a three-order tensor to a core tensor and three truncated orthogonal bases.

2.2 Fully Homomorphic Encryption

Homomorphic encryption is another kind of plan that permits particular sorts of operations to be performed on the cyphertext to acquire the scrambled result, of which the unscrambling is indistinguishable to the outcome straightforwardly processed by performing operations on the plaintext. Two completely homomorphic encryption plans [6, 11] are proposed utilizing perfect cross section and polynomial ring, separately. A Ring Learning with Errors (RLWE) base completely homomorphic encryption plan without bootstrapping is proposed , where a General Learning with Errors (GLWE) based plan is reported.The encryption plan bolsters the homomorphism of expansion and increase, which can be portrayed as takes after

Enc(m1) + Enc(m2) = Enc(m1 + m2);

Enc(m1 × m2) = Enc(m1) × Enc(m2): (3)

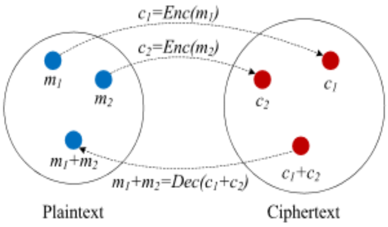


Fig. 2. Illustration of the homomorphic encryption.

Fig 2 shows homomorphic encryption of an expansion operation. Let m1, m2 be two components in the plaintext, c1, c2 in the ciphertext, and
c1 = Enc(m1)
,c2=Enc(m2), then
m1+m2 = Dec(Enc(m1)+Enc(m2)).

2.3 Lanczos Method

The Lanczos technique is effective for figuring the eigenvalues and eigenvectors of a meager symmetric lattice. It changes the lattice M with an orthogonal framework W, where W = [w1,. ,.wk] and WTW = I, to a tridiagonal grid as takes after

$$L = \begin{bmatrix} \alpha_1 & \beta_2 & & \\ \beta_2 & \alpha_2 & \ddots & \\ & \ddots & \ddots & \beta_k \\ & & \beta_k & \alpha_k \end{bmatrix}. \quad (4)$$

Comparing segments in the expression MW = WL, the tridiagonal lattice L can be produced via completing the cycle methodology

$$\alpha j = w^{T} M wj,$$

$$rj = Mwj - \alpha jwj - \beta jwj{-}1,$$

$$\beta j{+}1 = \|rj\|_2, \; wj{+}1 = rj/\beta j{+}1. \quad (5)$$

The parts of α, β, r can be logically ascertained. Give the eigenvalue disintegration of grid L a chance to be characterized as L = Q^QT, then the eigenvalues and eigenvectors of lattice M are ^ and WQ, separately. In the grid vector item is the much of the time called
direct change amid the Lanczos system.

3 PROBLEM DEFINITION AND SOLUTION FRAMEWORK

This area formalizes the issue of secure tensor disintegration on the bases of the completely homomorphic encryption plot, and gives a review of the proposed arrangement structure.

3.1 Problem Definition

Heterogeneous information comprise of unstructured information Du, semi organized information Dsemi, and organized information Ds. Give center a chance to indicate the center information including the center tensor S and the truncated orthogonal bases U1, U2,… .,UN, then the protected tensor disintegration issue can be formalized as

fr : {Enc(Du),Enc(Dsemi),Enc(Ds)} →Enc(T),
fd :Enc(T) →{Enc(S),Enc(U_1), …. , Enc(U_N)}:
(6)

In Eq. (6) the information representation capacity fr incorporates all scrambled information as a bound together figure tensor model (UCT), on which the disintegration capacity fd is performed to create the encoded center tensor and additionally the encoded truncated orthogonal bases.

As the decay operations are carried on the encoded information, the client's security are ensured. To ensure the rightness of the deterioration result Eq. (6) fulfills S = T×1U1T×2U2T … .×NUNT. As per the completely homomorphic encryption plot, the safe decay process fulfills the accompanying condition

Dec(sk; Eva(pk; Cfd ; Enc(T))) = Cfd (T); (7)

where Eva, Enc, Dec allude to the assessment, encryption,and decoding capacity, pk and sk signify the general population keyand private key, Cfd alludes to the boolean circuits of thetensor decay capacity fd characterized in Eq. (6).

The homomorphism can be ensured by performing expansion, subtraction, and duplication operations on the figure information amid the tensor deterioration process. Notwithstanding, new difficulties emerge when the nonhomomorphic operations, for example, square root and division are embraced in some writes of decay techniques, for instance, Lanczos-based calculation. A safe tensor decay calculation is proposed in this
paper to address these challenges.

For convenience, in the following sections this paper adopts the symbol Ψ^E to denote the cipher data ing to the plain data Ψ, namely $\Psi^E = Enc(\Psi)$. Therefore, the encrypted tensor $Enc(T)$ is denoted as T^E.

3.2 Overview of the Solution Framework

To address the problem defined above, this paper proposes a secure tensor decomposition approach based on the fully homomorphic encryption scheme. Fig. 3 provides an overview of the framework where the unstruc- tured, semi-structured, and structured data are encrypt- ed and represented as a unified tensor model, which is then securely decomposed to a core tensor multiplied with a certain number of truncated orthogonal bases. The four representative steps of the solution framework are summarized as follows.

1 Data Representation, Encryption and Submission: The heterogeneous data collected in the clients are represented as low-order sub-tensors using the method proposed in previous work then the sub-tensors are encrypted using the fully homo- morphic encryption scheme and the generated cipher results are submitted to the cloud for unifica- tion and decomposition. In Fig. 3, the unstructured video data V D, semi-structured XML document XD, and structured database DB are transformed to cipher low-order sub-tensors T^E_{VD},T^E_{XD},T^E_{DB} respectively.

2 Construction of Cipher Tensor: The generated sub-tensors T^E_{VD},T^E_{XD},T^E_{DB} respectively. are then embedded to a base tensor model Tbase ∈ RItim ×Ispa ×Iclt to generate a unified cipher tensor model TE using the tensor extension operation TE Tbase⇀×TEV D⇀×TEXD×TEDB the three orders Itim; Ispa; Iclt of the base tensor model denote the time, space and client characteristics.

3 Secure Tensor Decomposition: After unfolding theunified cipher tensor TE to matrices TE(1),…., TE(N),where N is the number of orders of tensorTE,thesymmetrization transformation is performed on each tensor unfolding to generate the symmetric matrix sym(TE(i)) = TE(i)(TE(i))T; 1 ≤ i ≤ N. The eigen vectors of the symmetric matrix sym(TE(i)) are corresponding to the left singular vectors of matrix TE(i). The Lanczos method is employed to perform the eigen value decomposition, namely,sym(TE(i)) = UEi ^EUEi)T. The cipher core tensor SE can be computed by applying Eq. (1) to the truncated bases UE1 ,…, UEN and the unified cipher tensor TE.

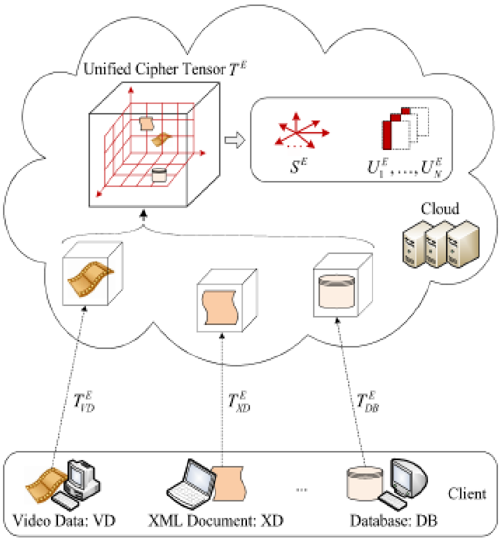


Fig. 3. Framework overview of the secure tensor decom- position approach.

4 Obtain the Plain Core Tensor and Bases: By decrypting the cipher core tensor and cipher truncated bases generated in Step 3, the plain core tensor S and plain truncated orthogonal bases U1,…., UN can be computed. As the homomorphism are supported during the secure tensor decomposition, the generated results are correct and are identical to that directly computed using the plain data. This paper focuses on Step 2 and Step 3, which correspond to the secure representation function fr a

4 LITERATURE SURVEY

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics**,** three service models, and four deployment models.

C. Gentry - We propose a fully homomorphic encryption scheme – i.e., a scheme that allows one to evaluate circuits over encrypted data without being able to decrypt. Our solution comes in three steps. First, we provide a general result – that, to construct an encryption scheme that permits evaluation of arbitrary circuits, it suffices to construct an encryption scheme that can evaluate (slightly augmented versions of) its own decryption circuit; we call a scheme that can evaluate its (augmented) decryption circuit bootstrappable.

Next, we describe a public key encryption scheme using ideal lattices that is almost bootstrappable. Lattice-based cryptosystems typically have decryption algorithms with low circuit complexity, often dominated by an inner product computation that is in NC1. Also, ideal lattices provide both additive and multiplicative homomorphisms (modulo a public-key ideal in a polynomial ring that is represented as a lattice), as needed to evaluate general circuits. Unfortunately, our initial scheme is not quite bootstrap- pable – i.e., the depth that the scheme can correctly evaluate can be logarithmic in the lattice dimension, just like the depth of the decryption circuit, but the latter is greater than the former. In the final step, we show how to modify the scheme to reduce the depth of the decryption circuit, and There by obtain a bootstrappable encryption scheme, with out reducing the depth that the scheme can evaluate. Abstractly, we accomplish this by enabling the encrypter to start the decryption process, leaving less work for the decrypter, much like the server leaves less work for the de-crypter in a server-aided cryptosystem.

L. Kuang, F. Hao, L. T. Yang, M. Lin, C. Luo, and G. Min - Variety and veracity are two distinct characteristics of large-scale and heterogeneous data. It has been a great challenge to ef_ciently represent and process big data with a uni_ed scheme. In this paper, a uni_ed tensor model is proposed to represent the unstructured, semistructured, and structured data. With tensor extension operator, various types of data are represented as subtensors and then are merged to a uni_ed tensor. In order to extract the core tensor which is small but contains valuable information, an incremental high order singular value decomposition (IHOSVD) method is presented. By recursively applying the incremental matrix decomposition algorithm, IHOSVD is able to update the orthogonal bases and compute the new core tensor. Analyzes in terms of time complexity, memory usage, and approximation accuracy of the proposed method are provided in this paper. A case study illustrates that approximate data reconstructed from the core set containing 18% elements can guarantee 93% accuracy in general. Theoretical analyzes and experimental results demonstrate that the proposed unified tensor model and IHOSVD method are efficient for big data representation and dimensionality reduction.

5. CONSTRUCTION ON CIPHER TENSOR VIA FULLY HOMOMORPHIC ENCRYPTION SCHEME ON CLOUD

This section illustrates the process of representing the heterogeneous data as a unified cipher tensor model via the fully homomorphic encryption scheme. New concepts and operations closely related to the cipher tensor model are introduced.

5.1 Cipher Tensor and Nil Element

In order to clearly describe the process of representing the unstructured, semi structured, and structured data as a unified cipher tensor model.

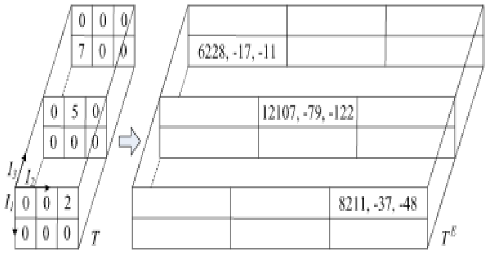


Fig. 4. A plain tensor and the corresponding cipher tensor.

5.2 Constructing a Unified Cipher Tensor Model on Cloud

In this paper, the heterogenous data are first represented and encrypted as cipher low-order sub-tensors on the clients, then they are submitted to the cloud for unification. To integrate all the cipher sub-tensors, a base tensor model is proposed, which is defined as Tbase ∈ RItim×Ispa×Iclt , where Itim; Ispa; Iclt refer to the time, space and client characteristics. The three orders serve as a basis to which various types of encrypted subtensors can be appended to generate a unified cipher tensor model.

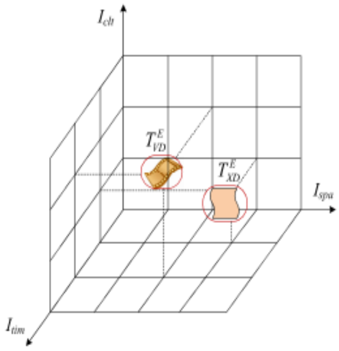


Fig. 5. Embedding two encrypted sub-tensors to the base tensor model on cloud.

5.3 Tensor Unfolding and Memory Storage Scheme

When the unified cipher tensor is generated, the next critical step is to obtain the tensor unfolding, which are then transformed to symmetric matrices. For sparse tensor, the Compressed Row Storage (CRS) method is employed to store the unfolded matrices. The CRS scheme is efficient for matrix-vector product and can reduce memory usage during tensor decomposition. Additionally, in order to decrease execution time of the secure tensor decomposition algorithm, the data-intensive application can employ $T^E(i)((T^E(i))T$ v) toperform the matrix-vector operation on the symmetric matrix of the i-mode tensor unfolding.

5.4 Cipher Tensor Representation Algorithm on Cloud

Based on the above mentioned methods, this paper proposes Algorithm 1 to represent the heterogeneous data as a unified cipher tensor (UCT) model on cloud.

Algorithm 1 Cipher Tensor Representation. TE =fr(Du; Dsemi; Ds)

Input:

The unstructured data Du, semi-structured dataDsemi, and structured data Ds.

Output:

The unified cipher tensor model TE.

1. Represent the local heterogeneous data as low-order sub-tensors, and encrypt them to cipher low-order sub-tensors on clients.
2. Upload the generated cipher sub-tensors to cloud.
3. Embed all the cipher sub-tensors to the base tensor model $T_{base} \in R_{Itim \times Ispa \times Iclt}$, and obtain the unified cipher tensor model TE.
4. Unfold the cipher tensor to matrices and generate the symmetric matrices for decomposition.

In Line 1 of the proposed Algorithm 1, the unstructured, semi-structured, and structured data are transformed to low-order sub-tensors, which are then encrypted using the fully homomorphic encryption scheme on clients. All the cipher sub-tensors are uploaded to cloud for unified representation. In this paper, the zero elements of the plain data are removed during the encryption procedure. The cloud embeds all the cipher sub-tensors to the base tensor model in Line 3 to obtain the unified cipher tensor model T^E. Line 4 generates the symmetric matrices of each cipher tensor unfolding for secure tensor decomposition.

6 EXISTING SYSTEM:

A tensor model is utilized to delineate the straight relations between the scalars, vectors, and different tensors. Tensor is a speculation of a network model, which is generally called multidimensional exhibit. It can adequately speak to the heterogeneous information as a succinct model with which the profitable data can be separated utilizing the High Order Singular Value Decomposition (HO-SVD) technique. As the HO-SVD strategy forces orthogonal limitation on the truncated vector bases, it is considered as an exceptional instance of the normally utilized TUCKER decay. HO-SVD has been received for information examination and information mining in numerous fields, for example, label suggestions and written by hand digit order.

The idea of completely homomorphic encryption was initially presented in 1978. The encryption plans reported in backings either expansion homomorphism or augmentation homomorphism. In any case, none of the can bolsters both operations in a solitary plan. Another methodology is introduced in which builds a plan equipped for completing both expansion and increase operations. It handles a discretionary number of increases however one duplication. In 1999, Gentry built a completely homomorphic encryption plot that can assess a discretionary number of increments and increases on the scrambled information. From that point on numerous studies have been performed with a specific end goal to display new effective completely homomorphic encryption plans

6.1 DISADVANTAGE EXISTING SYSTEM:

□ However, doing such sorts of errands on cloud may bring about a progression of security issues including loss of protection

□ limited number of operations of completely homomorphic encryption

□ less time many-sided quality, memory use, deterioration precision, and information security are given.

7. PROPOSED SYSTEM

This paper shows another processing approach which can safely decay the tensor model created from huge scale heterogeneous information. The real commitments are condensed as takes after

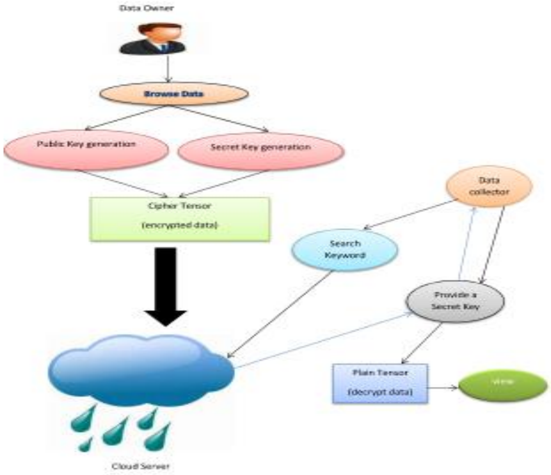
• We introduce an all encompassing structure to address the issue of secure tensor deterioration on cloud.

The structure not just permits us to use the effective computational capacities of the cloud, additionally guarantees information security amid the procedure of tensor decay.

• We present a Unified Cipher Tensor (UCT) model for heterogeneous information representation. The nitty gritty methods of how to scramble the low-arrange sub-tensors developed from heterogeneous information as figure partners utilizing the completely encryption plan, and how to insert them to a base tensor space to produce a brought together figure tensor model are represented in this paper.

• We propose to utilize the Lanczos technique to break down the created figure tensor model to a center tensor and a specific number of truncated orthogonal bases. A protected tensor deterioration calculation is planned in which the nonhomomorphic square root operations are evacuated amid the Lanczos method. Hypothetical investigations of the calculation as far as time many-sided quality, memory use, disintegration exactness, and information security are given.

7.1 ARCHITECTURE DIAGRAM



7.2 ADVANTAGES PROPOSED SYSTEM

Exploratory results show that the methodology can safely break down a tensor. With the headway of completely homomorphic encryption plan, it can be normal that the safe tensor decay approach can possibly be connected on cloud for protection safeguarding information preparing.

As the homomorphism are bolstered amid the safe tensor disintegration, the created results are right and are indistinguishable to that specifically registered utilizing the plain information.

as far as time intricacy, memory use, deterioration exactness, and information security are given. Some exceptionally preparatory tests are done to assess the execution of the displayed strategies. The outcomes bolster that the proposed methodology is doable and can clear a path for secure information preparing on cloud.

8 CONCLUSION

Planning to propose a productive methodology that can safely prepare substantial scale heterogeneous information, this paper formalizes the protected tensor decay issue, and proposes an all encompassing arrangement structure to address it. A bound together figure tensor model is introduced to coordinate all the scrambled low-arrange sub-tensors as a brought together model. Brief cases are accommodated representing the procedure of figure tensor development and unfurling. A Lanczos-based secure tensor disintegration calculation is presented, in which the non-homomorphic square establish operations in Lanczos system are expelled. Hypothetical examinations regarding time unpredictability, memory utilization, decay precision, and information security are given. Some exceptionally preparatory trials are done to assess the execution of the exhibited strategies. The outcomes bolster that the proposed methodology is practical and can clear a path for secure information handling on cloud.

REFERENCES

[1] P. Mell and T. Grance, “The NIST Definition ofCloud Computing (Draft),” NIST Special Publication,vol. 800, no. 145, p. 7, 2011.

[2] L. J. van der Maaten, E. O. Postma, and H. J. van den Herik, “Dimensionality Reduction: A Comparative Review,” J. Machine Learning Research, vol. 10, no. 1-41, pp. 66–71, 2009.

[3] J. Han and M. Kamber, Data Mining, Southeast Asia Edition: Concepts and Techniques. Morgan kaufmann, 2006.

[4] M. Kantardzic, Data Mining: Concepts, Models, Methods, and Algorithms. John Wiley & Sons, 2011.

[5] R. L. Rivest, L. Adleman, and M. L. Dertouzos, “On Data Banks and Privacy Homomorphisms,” Foundations of Secure Computation, vol. 4, no. 11, pp. 169–180, 1978.

[6] C. Gentry, “Fully Homomorphic Encryption Using Ideal Lattices,” in Proc. 41st Ann. ACM Symp. Theory of Computing, vol. 9, 2009, pp. 169–178.

[7] K. Lauter, M. Naehrig, and V. Vaikuntanathan, “Can Homomorphic Encryption be Practical?” Cryptology ePrint Archive, Report 405, 2011, http://eprint.iacr.org/2011/.

[8] T. G. Kolda and B. W. Bader, “Tensor Decompositions and Applications,” SIAM Review, vol. 51, no. 3, pp. 455–500, 2009.

[9] L. Kuang, F. Hao, L. T. Yang, M. Lin, C. Luo, and G. Min, “A Tensor-Based Approach for Big Data Representation and Dimensionality Reduction,” IEEE Trans. Emerging Topics in Computing, vol. 2, no. 3, pp. 280–291, 2014.

[10] L. De Lathauwer, B. De Moor, and J. Vandewalle, “A Multilinear Singular Value Decomposition,” SIAM J. Matrix Analysis and Applications, vol. 21, no. 4, pp. 1253–1278, 2000.

[11] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, “Fully Homomorphic Encryption Over the Integers,” in Advances in Cryptology–EUROCRYPT 2010. Springer, 2010, pp. 24–43.

[12] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, “Fully Homomorphic Encryption Without Bootstrapping,” in Proc. 3rd Innovations in Theoretical Computer Science Conference. ACM, 2012, pp. 309– 325.

[13] J. K. Cullum and R. A. Willoughby, Lanczos Algorithms for Large Symmetric Eigenvalue Computations: Vol. 1: Theory. SIAM, 2002, vol. 41.

[14] M. Gr¨ uning, A. Marini, and X. Gonze, “Implementation and Testing of Lanczos-based Algorithms for Random-Phase Approximation Eigenproblems,” Computational Materials Science, vol. 50, no. 7, pp. 2148–2156, 2011.

[15] Z. Bai, J. Demmel, J. Dongarra, A. Ruhe, and H. van der Vorst, Templates for the Solution of Algebraic Eigenvalue Problems: A Practical Guide. SIAM,

[16] N. P. Smart and F. Vercauteren, “Fully Homomor- phic Encryption with Relatively Small Key and Ciphertext Sizes,” in Public Key Cryptography–PKC 2010. Springer, 2010, pp. 420–443.

[17] I. Popovyan, “Efficient Parallelization of Lanczos Type Algorithms,” Tech. Rep., 2011.

[18] I. Flesch and R. Bisseling, “A New Parallel Ap- proach to the Block Lanczos Algorithm for Finding Nullspaces Over GF (2),” M.S Thesis, Department of Mathematics, Utrecht University, Utrecht, the Nether- lands, 2002.

[19] P. L. Montgomery, “Distributed Linear Algebra,” in Proc. 4th Workshop on Elliptic Curve Cryptography, 2000.

[20] Z. Jia and D. Niu, “A Refined Harmonic Lanc- zos Bidiagonalization Method and An Implicitly Restarted Algorithm for Computing the Smallest Singular Triplets of Large Matrices,” SIAM J. Sci- entific Computing, vol. 32, no. 2, pp. 714–744, 2010.

[21] Q. Ye, “Error Bounds for the Lanczos Methods for Approximating Matrix Exponentials,” SIAM J. Numerical Analysis, vol. 51, no. 1, pp. 68–87, 2013.