Efficient Scheduling Mechanisms for Secured Cloud Data Environment

S. Selvi, R. Sridevi

Abstract— ***Big Data has won heaps of intrigue in light of the tremendous degree it presents for a higher comprehension of the business and decision making strategy for an enterprise. There has been a broad scope of looks into happening far and wide on this to make the most out of it and entirely some of specialized stages are to be need to the analysis for enormous records . However, Scientists and organizations had the option to expand frameworks that could deal with the enormous measurements and perform investigation on it, the security segments remain immensely immaculate. And misfortune can be a reason for significant data loss while applying hybrid security. As if information changes, then it is not valuable. So here is a need to adopt proper scheduling mechanism in cloud computing to avoid process delay. This paper expounds some encryption strategies and proper scheduling mechanisms. Hyper elliptic curve cryptography (HECC) towards verified enormous record analyses is embraced here to describe with proper scheduling.***

Index Terms— ***Big data Analytics, HECC, Homomorphic Encryption and Public-Key Encryption (PKE.).***

I. INTRODUCTION

Big Data Analytics is a term portrayed for a fixed of unstructured, huge amount of data that maybe can't be dealt with or handled with the guide of the accessible regular database structures. The intention at the back of this is basically because of the monstrous arrangement of unstructured, confused, changed assortments of insights that constrains the handling capacity of the ordinary database models. The term transformed into first included by means of Roger Magoulas from O'Rielly media [1] to recognize the preparing capability of entangled and unstructured records by ordinary databases. The idea of huge statistics turns out to be clear in its definition as gave by means of Gartner Inc [2] in its 4V model is recorded.

Volume: The large amount of statistical data generated every single minute by way of various transactional processes and different facts generation strategies such as airline systems, on line social media imposes a extremely good deal of statistics to be saved, processed and retrieved. For an example, Facebook generates around 500 terabytes (TB) of facts every day.

Variety: The problem of dealing with facts and processing has now been more tough due to the numerous varieties of records being disposed. There are text data, photograph facts, video records, database documents, emails etc. All of which makes the facts processing, a tedious job. This is by and large, one in all the largest motives why the existing database solutions are not suitable for huge records evaluation and we want unique solutions to handle such records.

Velocity: This essentially displays the speed at which the information is being generated and dispersed over the net. With this era of internet and cellular computing, gaining access to statistics has grow to be a lot less complicated and therefore large amount of data also are being generated from this utilization. This introduces the need to control the quick growing real time records and additionally to be able to structure the information for evaluation.

Veracity: Veracity refers back to the trustworthiness of the statistical data. Every Data Analyst is aware of that there are inherent discrepancies in all of the records amassed. Big Data Veracity refers back to the biases, noise and abnormality in statistics. The facts being saved, and mined big to the problem being analyzed. Veracity in fact is the most important challenge while compares to such things as volume and velocity. In scoping out the large records the approach need to have is organization and companions paintings to assist maintain the facts smooth and strategies to maintain 'grimy facts' from gathering from systems.

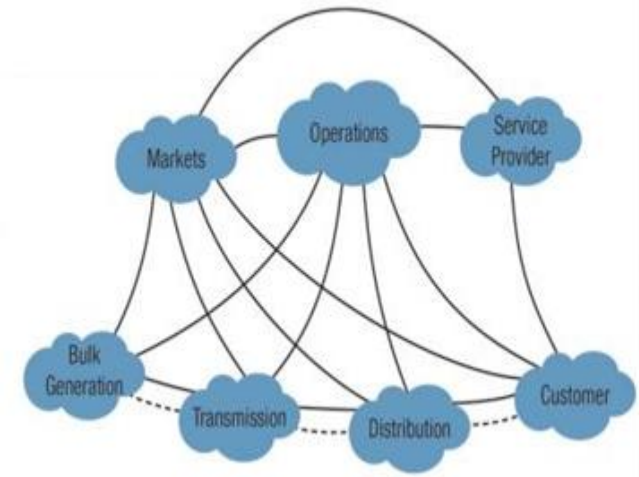

Figure 1: Big Data Access Framework (National Institute of Standards and Technology (NIST))

Evolving future skills will sooner or later be some distance beyond what we consider nowadays, regulatory steps and requirements are being installed place to maintain the Smart Grid in secured way. As further shrewd systems come to market, they will ought to preserve those key elements of hardware and software primarily based protection in thoughts if they are going in order to comply with the requirements

Revised Version Manuscript Received on 16 September, 2019.

S.Selvi, Professor , PSG College of Arts & Science, Coimbatore, Tamil Nadu, India.

R.Sridevi , Professor , PSG College of Arts & Science, Coimbatore, Tamil Nadu, India.

which might be entering play to serve the needs of the advancing strength marketplace.

Planning for distributed computing is a troublesome assignment in light of heterogeneity in resources and working frameworks. Planning is additionally a key test in the method for nature of administrations, buffering, transmitting and getting information in a system. Ideal resource designation in cloud chooses the number of resources need to distribute to a procedure to finish its execution. Distributed computing utilizes dynamic nature and it is should be planned cautiously. Cloud gives a few focal points to store information which expel prerequisite of storage capacity.

In this paper, the number one cognizance is on discussing the demanding situations and security problems associated with Big Data Analytics. The paper is established within the following way: Section 2 will deliver the security problems faced in big data analytics. Section 3 introduces scheduling mechanisms and encryption techniques. Section four and five talks approximately conclusion made and future development of secured Big Data Analytics.

II. SECURITY CHALLENGES IN BIG DATA

According to the Big Data Working Group on the Cloud Security there are, basically, 4 extraordinary elements of Big Data safety: infrastructure safety, information privacy, information management, and integrity and reactive protection. This division of Big Data protection into four essential subjects has additionally been utilized by the International Organization for Standardization with a purpose to create a security preferred for safety in Big Data. Figure 1 includes a scheme displaying the main subjects associated with challenges in Big Data.

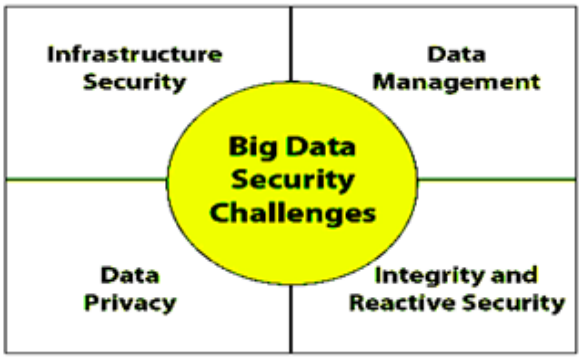

Figure 2: Big Data Security Challenges

Data are important to carrying out day by day activities, and also supporting the businesses, control to obtain their goals and make the best decisions on the basis of the data are extracted from them [3]. It is estimated that of all of the statistics in recorded human records, 90 percentages have been created inside the previous couple of years. In 2003, 5 hex bytes of information were created via humans, and this amount of information is created every two days at present [4]. This tendency towards increasing the extent and detail of the facts this is accrued with the aid of organizations will now not trade inside the near destiny, because the upward thrust of social networks, multimedia, and the Internet of Things (IoT) is generating an overwhelming glide of information [5]. We are dwelling within the era of Big Data. Furthermore, this fact is often unstructured, signifying that traditional systems are not able to analyzing it. Organizations are inclined to extract greater beneficial information from this excessive quantity and type of statistics [6]. A new analysis paradigm with which to examine and higher apprehend this information, consequently, emerged that allows to reap not most effective private, however additionally public, advantages, and this turned into Big Data [7].

Each new disruptive era brings new troubles with it. In the case of Big Data, these issues are related no longer only to the quantity or the style of records, but additionally to information, information privacy, and information security. These papers will consciousness at the subjects of Big Data privacy and security. Big Data now not only increases the scale of the demanding situations associated with privateers and security as they may be addressed in conventional safety management, however also create new ones that want to be approached in a new way [8]. As more records is saved and analyzed by way of businesses or governments, greater guidelines are had to cope with those worries. Achieving safety in Big Data has, therefore, end up one of the maximum critical barriers that would sluggish down the spread of technology; without good enough safety guarantees, Big Data will no longer achieve the required stage of believe [9]. Big Data brings big responsibility [10]. According to the Big Data Working Group at the Cloud Security Alliance agency there are, principally, 4 one of a kind aspects of Big Data security: infrastructure security, statistics privateness, facts control, and integrity and reactive security [11]. This division of Big Data safety into four major topics has additionally been used by the International Organization for Standardization as a way to create a protection fashionable for safety in Big Data. Figure 1 incorporates a scheme displaying the primary topics associated with protection in Big Data. As more facts is saved and analyzed with the aid of establishments or governments, extra regulations are had to cope with these issues. Achieving safety in Big Data has, consequently, grow to be one of the maximum important obstacles that would slow down the spread of technology; without good enough security ensures, Big Data will no longer acquire the required degree of consider [9]. Big Data brings large obligation [10]. According to the Big Data Working Group on the Cloud Security Alliance business enterprise there are, principally, four one of a kind factors of Big Data safety: infrastructure protection, statistics privacy, records management, and integrity and security [11]. This department of Big Data safety into fouressential subjects have also been utilized by the International Organization for Standardization on the way to create a security for safety in Big Data. Figure 1 contains a scheme displaying the principle topics related to protection in Big Data.

III. ELLIPIC AND HYPER ELLIPTIC CURVE CRYPTOGRAPHY

A. *Elliptic and Hyper Elliptic Curves*

Let K be a field of trademark ≠ 2, 3, and let $x^3 + ax + b$ (where a, b ∈K) be a cubic polynomial with no different roots. An elliptic curve over K is the arrangement of focuses (x, y) which fulfill the condition [4]

$y^2 = x^3 + ax + b$, together with single component meant by O and called the "point at infinity".

On the off chance that K is a field of trademark 2, at that point an elliptic curve over K is the arrangement of focuses fulfilling a condition of the type either

$y^2 + cy = x^3 + ax + b$ or

$y^2 + xy = x^3 + ax^2 + b$, together with a

" point at infinity" O.

In the event that K is a field of trademark 3, at that point an elliptic bend over K is the arrangement of focuses fulfilling a condition.

$y^2 = x^3 + ax^2 + bx + c$, together with a " point at infinity" O.

B. *Hyper Elliptic Curve Cryptography*

It is a big measure of consideration since it offers some benefits over different public key cryptosystems, as an instance, RSA. With a better protection for every key piece than RSA, HECC takes into consideration a comparable degree of safety with a littler key size [13]. Public key cryptography [14] may be applied to offer the administrations of Key foundation, computerized marks, and Encryption. In present day applications, public key primitives are applied to present these types of three administrations. For the encryption and verification of expansive records streams, one uses symmetric key calculations for the reason that public key calculations are typically talented. Computerized marks were a major thrust in the back of the utilization of public key calculations. They deliver trustworthiness, sender validation and additionally non-disavowal. Along those lines, the sender of a message cannot ward off the introduction from claiming a message which may be crucial. Since 1976, 3 awesome versions of public key cryptosystems of pragmatic importance have evolved specifically

i) Cryptosystems in view of the trouble of number factorization.

ii) Solving the Discrete Logarithm (DL) issue in limited fields (e.g., Diffe Hellman key

trade or Advanced Signature Algorithm) and

iii) The DL issue in the gathering of mathematical curves over a limited field. (e.g., Elliptic

Curve and Hyper Elliptic Curve Cryptosystems (HECC) are the most understood sorts.

HECC are a hypothesis of Elliptic Curve Cryptosystems (ECC) and have been encouraged for cryptographic programs in 1988 by means of Koblitz. Hyper elliptic curve cryptosystems had been extensively taken into consideration not just via the discover organization additionally in enterprise [15].

A. *$a_A \in_R N$ [choose a prime (a_A) at random in N]*

A. P_A ← [a_A] D [The form of PA is (u(x),v(x)) representation which is referred to as Mumford representation]

B *return P_A and a_A*

In step A, arbitrary prime variety generation is given. Probabilistic trial of Robbin-Miller or the deterministic trial of AKS can be followed. Be that as it may, exceptional seems into have tested that it requires exponential investment to determine the given tremendous variety is top or no longer using AKS calculation.

C. *Mumford Notations*

A hyper elliptic curve C: y2 + h(x)y = f(x), Each nontrivial divisor class over the field K can be spoken to through Mumford portrayal (u(x), v(x)) [MUM1985], in which u(x) and v(x), u, v K[x], are excellent match of polynomials by fulfilling the necessities of u is monic.

deg v <deg u g

u | v2 + vh - f

Operations can be completed on these hyper-elliptic curves. Points of interest can be had from [16], [17], [18].

D. *Homomorphic Encryption*

In conceptual variable based totally math, a homomorphism is a structure-safeguarding map among two arithmetical systems, as an example, groups.

Set G, together with an operation ○ (referred to as the group regulation of G) that consolidates any two additives a and b to border every other component, indicated a ○ b.

To qualify as a set, the set and operation, (G; ○ı), need to satisfy 4 stipulations known as the group maxims:

• Closure: For every of the a; b in G, the outcome of the operation, a○ b, is additionally in G.

• Associativity: For every of the a; b, and c in G,

(a ○ b) ○ c = a○ (b○ c).

• Identity thing: There exists a component e in G, with the give up aim that for every component a in G, the balance

e ○ a = a○ e = a holds. Such a factor is tremendous, and therefore one talks approximately the character aspect.

• Inverse thing: For every a in G, there exists an element b in G with the stop goal that a○ b =b ○ a = e, where in e is the character element. The identity of a collection G is regularly composed as 1.

The result can also depend on upon the request of the operands. In other words, the end result of joining thing a with issue b require now not yield the identical come about as consolidating aspect b with component a; the condition a ○ b= b○ a won't constantly be valid. This circumstance dependably holds inside the accumulating of entire numbers below enlargement,

for the reason that a + b= b + a for any two numbers (commutativity of enlargement). Groups for which the commutative circumstance a○ b= b○ a dependably holds are known as abelian group.

Given two gatherings (G,) and (H, ○), a gathering homomorphism from (G ,)to (H, ○) is a capacity f : G H with the end goal that for all g and g' in G it holds that f(g g')= f(g ○ g')..

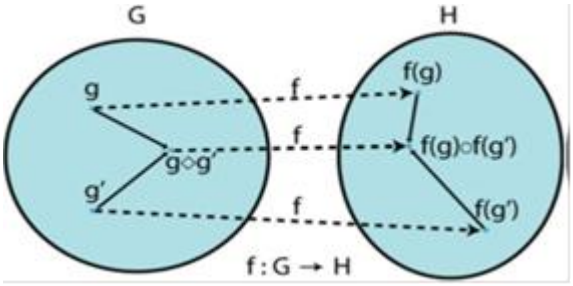

Figure3: Group homomorphism

Let (P, C, K, E ,D) be an encryption plot, in which P,C are the plaintext and ciphertext spaces, K is the key space, and E,D are the encryption and unscrambling calculations. Accept that the plaintexts frames a group (P,) and the ciphertext frames a group (C, ○), at that factor the encryption calculation E is a manual from the institution P to the group C, i.e., Ek : P → C , where ok € K is both a personal (in a private key cryptosystem) or public key (in an public key cryptosystem). For each of the a and b in P and k in K,

ifEk(a) ○ Ek(b) = Ek(a ◊ b) the encryption plot is homomorphic.

homomorphic operations are conveyed to get the resultant figure C. The customer utilizes homomorphic operations to check C in the cloud prior to data analysis. Hence hybrid encryption is utilized for high security and validation for receiving data before data analysis.

IV. SCHEDULING TECHNIQUES& RESULTS

Fundamental strategies are utilized to plan yet new scheduling systems can be accomplished essential planning technique based on client necessity. Fundamental scheduling strategies are appeared inFigure 4.

i. First Come First Serve:

First Come First Serve (FCFS) is an essential planning method utilized in distributed computing. FCFS deals with the premise of first procedure enter in the line and execute first. It fills in as a water supply pipe in which water enters from one end and exit from opposite end. Same work in cloud, as parcel transmitted by client from one end and got from opposite end in a similar request as they transmitted. Distributed computing utilize this booking strategy to transmit information as parcels as they are gotten by switch at sender end and got on other switch end. At that point they are reacted by the goal end. This is the most straightforward technique and lower cerebral pain in booking. This strategy is best where information is of little size. It is in such a case that information is of little size then it executes quick and no starvation happens.

ii . Priority Scheduling:

As the downside of starvation in FCFS, new planning technique required to keep away from starvation. Need Queue (PQ) stays away from procedures to go starve. For this need is relegated to process based on their necessity by client.

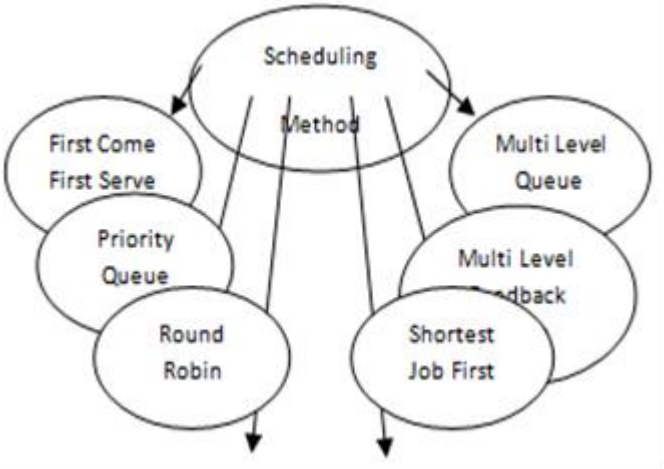

Figure 4. Scheduling Method

Client allots need to forms and most noteworthy need procedure executes first and the least need procedure execute in the last. It is same like human, as VIP (Very Important Person) get most noteworthy need and IP (Important Person) get medium need and normal individual get low need in road turned parking lot. By one way or another starvation happens for low need process however they execute in light of the fact that VIP and IP are less.

iii. Round Robin Scheduling:

Starvation isn't completely comprehended by FCFS and PQ. To take care of this issue another technique named Round Robin (RR) is utilized. Distributed computing utilizes this technique to transmit information. In this a period quantum is utilized and each procedure executes in the given quantum. In the event that procedure is of little quantum, at that point it's finished in this quantum. It gives procedures to go starve. Based on client necessity this planning strategy can be adjusted to get new booking.

iv.Shortest Job First Scheduling:

Shortest Job First (SJF) scheduling is best where little size procedure needs to execute first. This scheduling technique is best everlastingly to execute forms however as the planning relies upon the premise of client necessity some place it isn't appropriate. As on account of continuous based application, video and voice, they have to settle first. In any case, SJF chips away at the premise of most brief execution time of procedure and all things considered PQ booking strategy is best in which need is set to high to constant application in distributed computing.

V. RELATED WORK

R. Raju and R. G. Babukarthik portray limiting the make length utilizing highbrid calculation for distributed computing. In this paper they proposed half and half calculation which consolidate focal points of ACO and Cucko search [21]. Make range or fruition time can be diminished with assistance of crossover calculation.

PriyaR.Lodha and AvinashP.Wadhe they portray various kinds of work process planning calculation in distributed computing. Correlation is made based on working as for asset sharing, part client level and framework level [20]. This paper helps in determination of best scheduling technique which beat execution time.

LjiljanaTrazkovic depicts execution examination of scheduling disciplines. He utilizes OPNET Modeler to break down various lining systems based on packetl transmission and packet loss [22].

VI. CONCLUSION

Higher security is offered to the cloud information by using listed security techniques. These techniques plays computation at the encrypted report stored within the cloud which running on various scheduling algorithms, in turns, returns the encryption of addition or multiplication of authentic files. The scheme presented is easy and at ease because the HECC and Homomorphic encryption is used to implement the scheme. The scheme shops the encrypted files on a far away cloud space but the cloud space can't see the unique message. The cloud server does a few computations on saved documents and returns the computed documents to the authentic user for analytical purposes. Here a security evaluation made and showed the secured and effective scheduling algorithm. The protection of this proposed scheme relies upon the unbreakable keys produced with HECC.

REFERENCES

1. Discussion on Big data by Roger Magoulas, http:// strata. oreilly.com /2010/01/roger- magoulas- on - big- data.html
2. Gartner, Big Data Definition, http://www.gartner.com/ it-glossary/big-data/, accessed in September, 2013
3. Mayer-Schönberger, V.; Cukier, K. Big Data: A Revolution that Will Transform How We Live, Work, and Think; Houghton Mifflin Harcourt: Boston, MA, USA, 2013.
4. Sagiroglu, S.; Sinanc, D. Big data: A review. In Proceedings of the 2013 International Conference on Collaboration Technologies and Systems (CTS), San Diego, CA, USA, 20-24 May 2013; pp. 42-47.
5. Hashem, I.A.T.; Yaqoob, I.; Anuar, N.B.; Mokhtar, S.; Gani, A.; Ullah Khan, S. The rise of "big data" on cloud computing: Review and open research issues. Inf. Syst. 2015, 47, 98-115.
6. Sharma, S. Rise of Big Data and related issues. In Proceedings of the 2015 Annual IEEE India Conference (INDICON), New Delhi, India, 17-20 December 2015; pp. 1-6.
7. Eynon, R. The rise of Big Data: What does it mean for education, technology, and media research? Learn. Media Technol. 2013, 38, 237-240.
8. Wang, H.; Jiang, X.; Kambourakis, G. Special issue on Security, Privacy and Trust in network-based Big Data. Inf. Sci. Int. J. 2015, 318, 48-50.
9. Thuraisingham, B. Big data security and privacy. In Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, San Antonio, TX, USA, 2-4 March 2015; pp. 279-280.
10. Rijmenam, V. Think Bigger: Developing a Successful Big Data Strategy for Your Business; Amacom: New York, NY, USA, 2014.
11. Big Data Working Group; Cloud Security Alliance (CSA). Expanded Top Ten Big Data Security and Privacy. April 2013. Available online: https://downloads.cloudsecurityalliance.org/ initiatives/bdwg/Expanded_ Top_Ten_Big_Data_ Security_and_ Privacy_Challenges.pdf
12. Mrs. M.T.Wankhede-Barsgade, Dr. S. A. Meshram , "Comparative Study of Elliptic and Hyper elliptic Curve Cryptography in Discrete Logarithmic Problem ", IOSR Journal of Mathematics (IOSR-JM) e-ISSN: 2278-5728, p-ISSN:2319-765X. Volume 10, Issue 2 Ver. V (Mar-Apr. 2014), PP 61-63 www.iosrjournals.org www.iosrjournals.org
13. RamachandranGanesan , Mohan Gobi , and KanniappanVivekanandan; A Novel Digital Envelope Approach for A Secure E-Commerce Channel, International Journal of Network Security, Vol.11, No.3, PP.121-127, Nov. 2010
14. DrM.Gobi and D.Kannan," A Secured Public Key Cryptosystem for Biometric Encryption", International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014
15. Ms.S.Selvi,Dr.R.Ganesan, "An efficient Access Control Protocol for cloud data security using Hyper Elliptic Curve Cryptography" - IRACST - International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.6, No 4, July-August 2016
16. Menezes A J, Yi Hong Wu, Robert J Zuccherato (1996)," An elementary introduction to hyper elliptic curves", Technical Report CORR 96-19, University of Waterloo, Ontario, Canada, November 1996.
17. Lange T (2002), Efficient arithmetic on genus 2 hyperelliptic curves over finite fields via explicit formulae", Cryptology ePrint Archive: Report 2002/121, 2002.
18. Stallings W (2002), "Cryptography and Network Security: Principles and Practice", 2nd Edition, Pearson Education, 2002.
19. Improving Cloud Data Security using Hyper Elliptical Curve Cryptography & Steganography' S.Selvi, M.Gobi International Journal for Scientific Research & Development| Vol. 5, Issue 04, 2017 | ISSN (online): 2321-0613.
20. Priya R. Lodha and Avinash P. Wadhe,"Study of Different Types of Workflow Scheduling Algorithm in Cloud Computing" IJARCSEE International Journal of Advance Research in Computer Science and Electronics Engineering ISSN: 2277-9043 Volume 2, Issue 4, April 2013.
21. R.Raju and R. G. Babukarthik," Minimizing the Make span Using Hybrid Algorithm for Cloud Computing" 3rd IEEE International Advance Computing Conference(IACC) 978-1-4673-4529-3/12, 2013.
22. LjiljanaTrazkovic," Performance Analysis Of Scheduling Disciplines" SPRING ENSC894: Communication Network, 2012.