Security System for Big Data Cloud Computing Using Secure Dynamic Bit Standard

Faiz Akram

Abstract Big data (BD) is a high-volume resource that requests savvy and imaginative types of data handling for improved knowledge revelation, dynamic, and procedure streamlining. CC gives a solid, deficiency open-minded, and adaptable condition to the enormous information appropriated the board frameworks. The Secure Dynamic Bit Standard (SDBS) calculation gives the security through two unique keys, for example, the ace key and meeting key created by cloud service providers (CSP). The SDBS calculation contains the three distinctive key lengths, for example, 128 bits, 256 bits, and 512 bits. The length of the ace key and meeting key is arbitrarily created during the encryption procedure. CSP scrambles the ace key with the meeting key and sends the encoded ace key and meeting key to the infor-mation suppliers on demand. The information supplier unscrambles the ace key with the meeting key and encodes the information record with the decoded ace key. This strategy will decrease the most extreme number of unauthenticated and unapproved clients in a huge information cloud.

Keywords Cloud computing (CC) · Cloud service provider (CSP) · Secure Dynamic Bit Standard (SDBS)

1 Introduction

Cloud computing (CC) has numerous applications, for example, empowering access to costly applications at no cost, lessening both foundation and running costs of PCs and programming as there is no requirement for any establishment. Clients can put the information at anyplace [1]. All clients are required to connect with a framework, state the Internet. CC began as an instrument for relational figuring, however now it is generally utilized for getting to programming on the web, online capacity without stressing over foundation cost, and preparing power. Associations can offload their information technology (IT) foundation in the cloud and get entrance. Not just private

F. Akram (✉)
Faculty of Computing and Informatics, Jimma Institute of Technology, Jimma University, Jimma, Ethiopia
e-mail: akram.faiz@ju.edu.et; akram.faiz@gmail.com

V. Bindhu et al. (eds.), *International Conference on Communication, Computing and Electronics Systems*, Lecture Notes in Electrical Engineering 733,
https://doi.org/10.1007/978-981-33-4909-4_1

associations are moving to distributed computing, yet the legislature is additionally moving a few pieces of its IT framework to the cloud. Huge information includes the advanced information from a few computerized sources which contain sensors, scanners, numerical displays, recordings and cell phones, digitizers, Internet, messages, and interpersonal organizations which are expanding the information rate.

and enormous information are conjoined [2, 3]. BD gives clients the capacity to utilize merchandise figuring to process dispersed questions over numerous datasets and return resultant sets in an opportune way. CC gives a class of dispersed information handling stages. Huge information sources from the cloud and Web are put away in a conveyed flaw lenient database and handled through a programming model for huge datasets with an equal disseminated calculation in a group [4]. The multifaceted nature and assortment of information types are handling the capacity to perform an investigation on huge datasets. CC foundation can fill in as a successful stage to address the information stockpiling required to perform an enormous information examination. CC is associated with another example for the arrangement of registering foundation and enormous information handling strategy for a wide range of assets accessible in the cloud through information examination.

A few cloud-based advancements need to adapt to this new condition since managing BD for simultaneous handling has gotten progressively confounded. MapReduce is a genuine case of BD handling in a cloud domain; it permits the preparation of a lot of datasets put away in equal in the group. Group processing displays great execution in conveyed framework situations, for example, PC force, stockpiling, and system correspondences. Moreover, the capacity of bunch figuring is to give a cordial setting to information development. Database management systems (DBMSs) are viewed as a piece of the currently distributed computing engineering and assume a significant job to guarantee the simple change of utilizations from old venture foundations to new cloud framework designs [5]. The weight for associa-tions to rapidly receive and execute advances, for example, CC, to address the test of large information stockpiling and preparing requests involves unforeseen dangers and results [6].

2 Security in BD-CC

Big data cloud computing (BD-CC) transforms into a valuable and standard plan of action in light of its engaging segments. Notwithstanding the current advantages, the past segments also bring about authentic cloud-specific security issues. The all-inclusive community concern is security in the cloud, and the clients are deferring to trade their business to the cloud. Security issues have been the prevention of the improvement and expansive use of CC [7]. Understanding the security and assurance chances in CC, making rich and powerful arrangements are essential for its thriving, regardless of the way that mists empower clients to avoid fire up costs, lessen working expenses, and unite their speed by rapidly getting administrations and infrastructural assets when required.

In publicizing and business, the greater part of the ventures utilizes large information; however, the key properties of security may not be executed [8]. On the off chance that security penetrates happens to BD, it would result in much more genuine lawful repercussions and reputational harm than at present.

In this new time, numerous organizations are utilizing the innovation to store and examine petabytes of information about their organization, business, and their clients. For making BD secure, procedures, for example, encryption, logging, nectar pot recognition must be fundamental. In numerous associations, the organization of BD for misrepresentation location is alluring and helpful. The test of recognizing and forestalling propelled dangers and noxious interlopers must be explained utilizing large information style examination. The difficulties of security in CC conditions can be classified into an organized level, client verification level, information level, and conventional issues [9].

The difficulties can be sorted under a system-level arrangement with organizing conventions and system security, for example, disseminated hubs, and appropriated information, and inter hub correspondence.

The difficulties can be classified under client verification level arrangements with encryption or unscrambling procedures, validation techniques, for example, authoritative rights for hubs, verification of utilizations and hubs, and logging.

The difficulties can be classified under information level arrangements with infor-mation honesty and accessibility, for example, information security and disseminated information.

The difficulties that can be ordered under the general level are customary security apparatuses and utilization of various advancements.

3 Security Attacks

Distributed computing relies for the most part upon the structure of the current system, for example, metropolitan area network (MAN), wide area network (WAN), and local area network (LAN). System-level security assaults might be deliberately made by outside clients or by a malevolent insider staying between the client and the cloud service providers (CSP) and endeavoring to encroach upon the information to or from the cloud. This segment will endeavor to focus on the system-level security assaults and their possible countermeasures to ensure genuine information secrecy and dependability [10, 11].

3.1 Space Name System (DNS)

Attacks on the Internet, since reviewing a framework described by the numbers is troublesome, the aggressors are made to do with names. The Internet Protocol plays a remarkable role over the Internet related to the PC. The names of the DNS

automatically change concerning the IP addresses utilizing a disseminated database schema. Web DNS servers are dependent upon various types of attacks, for example, space catching, ARP store hurting, and man-in-the-middle attacks. A discussion of these attacks was found underneath.

3.2 Space Hijacking

Domain capturing alludes to changing the name of an area without the data or consent from the area owner or producer. Area seizing engages intruders to get corporate data and play out the unlawful development, for instance, phishing, where a site is superseded by a similar segment that records private data. Another arrangement is using the Extensible Provisioning Protocol (EPP) that is used by various area vaults. EPP utilizes an approval code gave uniquely to the space registrant as a safety effort to envision unapproved names advancing.

3.3 IP Spoofing Attack

The attacker buildups across unapproved admittance to a PC by proposing the PC to have the intention of undergoing through heavy traffic are known as IP mocking. Various attacks are employed by IP caricaturing, for instance, denial of service assault [12].

3.4 Disavowal of Service (DoS) Attacks

The inspiration driving these assaults is making the physical system and PC assets out of reach. During the DoS attack, the attacker submerges the disaster with a broad number of software packages over short intervals. DoS aids to identify distinguishing the devouring data between the systems. The assailant practices a false IP address as the source IP address to hold the interruption of the DoS. Furthermore, it is conceivable to the aggressor to utilize distinctive traded off machines that need to begin at presently seized to attack the misfortune machine in the interim. This kind of interruption handled by the DoS is known as the distributed DoS [13].

3.5 Transmission Control Protocol Synchronize (TCP SYN) Flooding Attack

While possessing situations like the DoS attack, the hackers employ the TCP SYN packages to pervert the machines. These kinds of attacks will certainly damage the restrictions of the three-course handshake when maintaining the half-open affiliations. A man-in-the-middle (MITM) attack is an overall term for when a culprit positions himself in a discussion between a client and an application by either to snoop or to imitate one of the gatherings, causing it to show up as though an ordinary trade of data is in progress. The bundle filtering is a method adopted to reduce the IP ridiculing that has been executed with the assistance of beginning stage confirmation systems, solid encryption, and a firewall [14, 15].

4 Methodology

SDBS have three-piece levels, for example, 128 bits, 256 bits, and 512 bits. At whatever point the information supplier needs to transfer an information record to the cloud, any of the bit levels is chosen haphazardly and it will get changed over into bytes. Because of byte esteem, CSP will produce the ace key and a meeting key utilizing an irregular generator. The ace key is scrambled by the meeting key, and both the encoded ace key and the meeting key will be sent to the information supplier.

The meeting key will be utilized to unscramble the ace key, and the ace key is utilized to scramble the information document. The encoded information document will be transferred to the huge information cloud server alongside the proof of ownership which is created by CSP. On the off chance that an information client needs to download an information document from the large information cloud server, according to popular demand, the CSP will send the encoded ace key and the meeting key alongside the scrambled information record to the information client after one-time password (OTP) check.

At that point, utilizing this meeting key the ace key will be unscrambled, and utilizing the ace key the information record will be decoded and put away in the arrangement of the information client. SDBS calculation is a novel calculation that has three different guidelines with ten rounds for 256-bit keys, eight rounds for 128-bit keys, and 12 rounds for 512-bit keys. The round contains different activities like substitution, adjustment, and change of the info plaintext into the yield figure text (Fig. 1).

The encryption process of SDBS algorithm with the 128-bit standard is shown in Fig. 2.

The plain content called a state cluster 'S' has four lines of bytes. Each line of a state contains N_b quantities of bytes, where N_b fluctuates for these three guidelines.

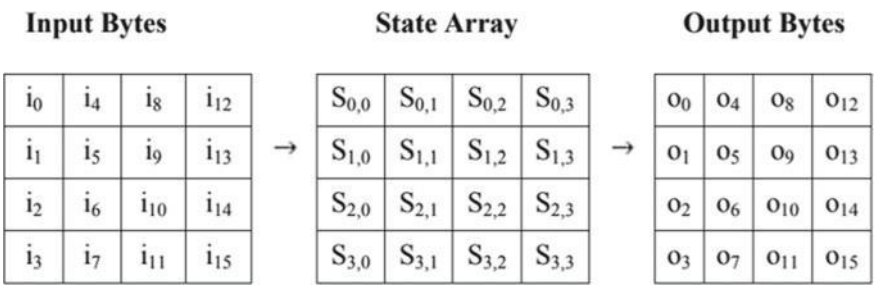

Fig. 1 Input bytes, state array, and output bytes

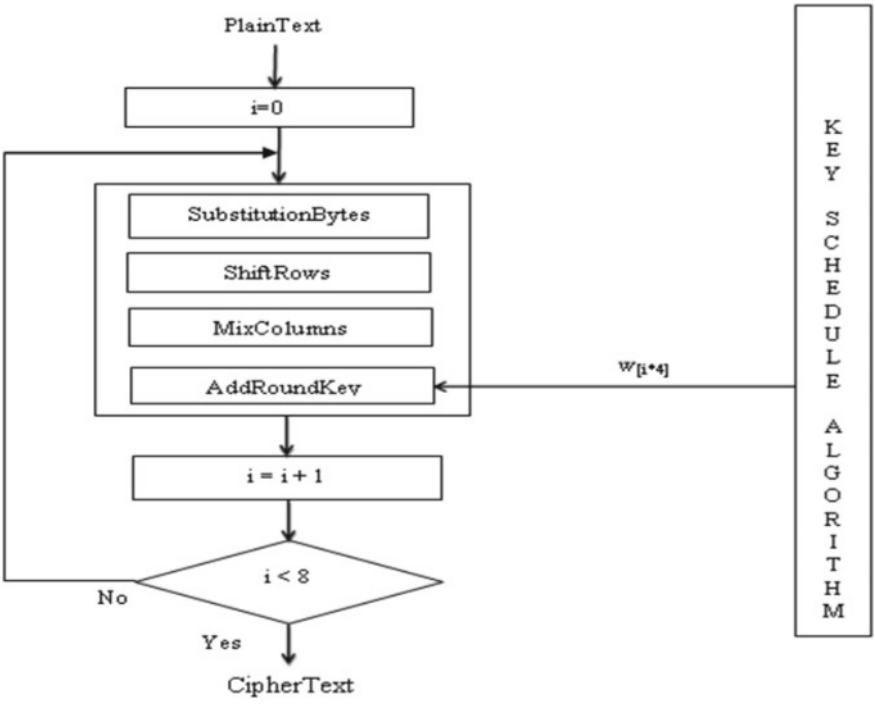

Fig. 2 SDBS encryption process for 128-bits standard

For the 128-bit standard, the estimation of N_b is 4, for the 256-bit standard, the estimation of N_b is 8, and for the 512-bit level, the estimation of N_b is 16.

The variety of information bytes appeared as i_0, i_1, …, i_{15} and the variety of yield bytes is spoken to by o_0, o_1, …, o_{15} as appeared in Fig. 1.

Decoding process: In SDBS unscrambling process, the information supplier must login and afterward select an information record, and the information client needs to download. Before downloading the information document, the information client

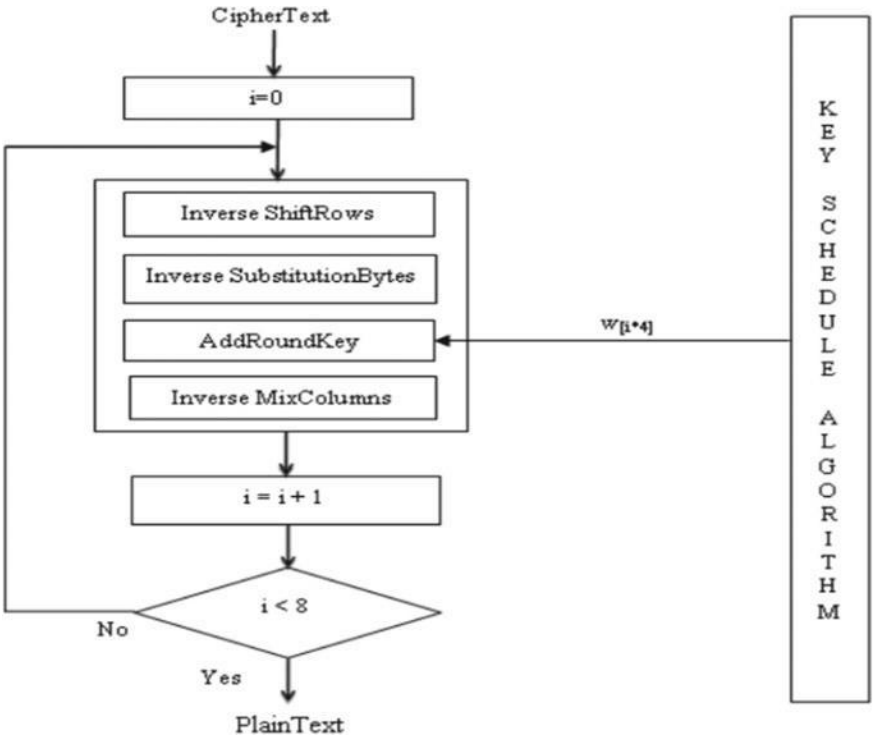

Fig. 3 SDBS decryption process of 128-bits standard

sends the solicitation to the CSP to get the ace key and meeting key. CSP encodes the ace key with the meeting key and sends to the information client.

OTP is additionally sent by the CSP to the information client's email id or versatile no. On the off chance that the entered OTP is substantial, at that point the encoded information document will be downloaded from the cloud, and the decoded ace key with the meeting key is utilized to begin the unscrambling procedure. At long last, the decoded record is put away into the framework (Fig. 3).

5 Results

The proposed method is performed and tried on a workstation with the following hardware specifications like 8 GB RAM, Windows 7 (64-bit) operating system, Intel i7 processor within the cloud storage (dropbox distributed storage) (Table 1).

The exhibition of SDBS calculation could be dissected by two sorts of bound-aries which are encryption time and decoding time. The encryption time is measured by the time taken to complete the encryption process along with the record size.

Table 1 Role and operation of multilevel SDBS

Role	Operation
Data Provider (DP)	Encrypt Data File
	Upload Data File
Data User (DU)	Download Data File
	Decrypt Data File
Cloud Service Provider (CSP)	Authenticate—Checking User Name and Password
	Authorize—Checking Credentials of the User
	Key Generation, OTP Generation, PoW Generation
	Block Unauthorized User

And the decryption time is measured by the time taken to complete the decryption process along with the record size. The genuine portrayal of SDBS 128-bits standard encryption time and unscrambling time-dependent on record size is spoken to underneath.

Figure 4 portrays the presentation of encryption time and unscrambling time versus record size in conspire 4. The diagram is completely based on the encryption time and document size. The encryption or unscrambling time of the proposed scheme 4 is less time when contrasted and different methods conspire 1, plot 2, and plan 3. This strategy took 2.56 ms for encoding 1 GB information document, likewise the 24 GB information record took 12.1 ms for encryption. From Fig. 4, 15, 1 GB information record took 2.35 ms for decoding; additionally, the 24 GB information document took 11.72 ms for unscrambling.

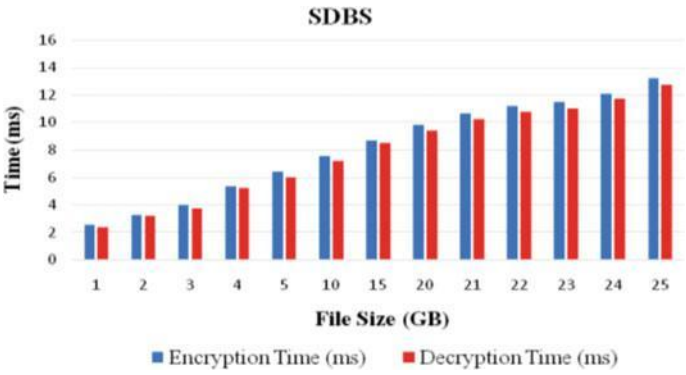

Fig. 4 Performance of SDBS 128-bits standard

6 Conclusion

The proposition gave a point by point prolog to the security framework in big data cloud computing. Big data distributed storage limits and applications are clarified. The conceivable outcomes of various assaults are portrayed in detail. In this article, information moved to the big data cloud has been finished by the information supplier. The proposed framework has high information respectability and information stockpiling without information misfortune. Before the information has been transferred into the capacity region, a high secure calculation called Secure Dynamic Bit Standard is been utilized. Big data investigation report assists by distinguishing each datum supplier and information client use of document size, encryption time or decoding time, and transfer time or download time.

References

1. Nahar AK, Mongia K, Kumari S (2018) Cloud computing and cloud security. Int J Res Adv Eng Technol 4(1):1–8
2. AshwinDhivakar MR, Ravichandran D, Dakha V (2015) Security and data compression in cloud computing using BlobSeer technique. In: National conference on cloud computing and big data, vol 1(12), pp 201–203
3. Ateniese G, Fu K, Green M, Hohenberger S (2006) Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Trans Inf Syst Secur 9(1):1–30
4. Attrapadung N, Herranz J, Laguillaumie F, Libert B, De Panafieu E, Ràfols C (2012) Attribute-based encryption schemes with constant size cipher texts. Theoret Comput Sci 422:15–38
5. Awodele O, Izang AA, Kuyoro SO, Osisanwo FY (2016) Big data and cloud computing issues. Int J Comput Appl 133(12):35–47
6. Bachhav S, Chaudhari C, Shinde N, Kaloge P (2016) Secure multi cloud data sharing using key aggregate cryptosystem for scalable data sharing. Int J Comput Sci Inf Technol 3(1):19–27
7. Balasubramanian N, Balasubramanian A, Venkataramani A (2009) Energy consumption in mobile phones: a measurement study and implications for network applications. In: Proceedings of the 9th ACM SIGCOMM conference on internet measurement conference, vol 1(5), pp 280–293
8. Bavisi S (2018) Computer and information security handbook. Morgan Kaufmann Publication, Elsevier Inc., pp 375–341
9. Bhadauria R, Chaki R, Chaki N, Sanyal S (2011) A Survey on security issues in cloud computing. IEEE Commun Surv Tutor 3(16):1–15
10. Bisong A, Rahman M (2011) An overview of the security concerns in enterprise cloud computing. Int J Netw Secur Appl 3(1):30–45
11. Hemalatha M (2012) Cloud computing for academic environment. Int J InfCommunTechnol Res 97–101
12. Mathew S (2012) Implementation of cloud computing in education—a revolution. Int J Comput Theory Eng 473–475
13. Kaur M, Singh H (2015) A review of cloud computing security issues. Int J AdvEngTechnol (IJAET), pp 397–403
14. Gaikwad BP (2014) A critical review on risk of cloud computing in commercial. Int J Innov Res Comput CommunEng 1–8
15. Ahmed ES, Saeed R (2014) A survey of big data cloud computing security. Int J Comput Sci SoftwEng (IJCSSE), pp 78–85