The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1989 – 2002

Privacy Preservation Techniques for Secure Data Broadcasting using in Distributed Environments

Rohit Ravindra Nikam[1], Rekha Shahapurkar[2]

[1]*Computer Science and Engineering Department, Oriental University, Indore, Madhya Pradesh, India*

[2]*Computer Science and Engineering Department, Oriental University, Madhya Pradesh, Indore, India*

[1]Rohitnikam3000@gmail.com, [2]rekhashahapurkar@orientaluniversity.in

Abstract : This Data security and privacy are essential things nowadays due to a large amount of sensitive data broadcasting on social media websites. Most of Internet of Things (IoT) and health care applications having quite challenges to achieve privacy preservation when number of distributed resources has involved during the data broadcasting. In this paper, we proposed a distributed data analysis and privacy preservation framework. In this paper, we introduced numerous privacy preservation techniques during data distribution to achieve high privacy. Some traditional methods, data anonymization, generalization, random permutation, specialization, top-down and bottom-up data generalization, fingerprint insertion etc., are also evaluated on extensive data when distributing with multi parties: the proposed one-way hashing privacy, XOR operation for generating multiple secure copies. First, we develop a few dynamic policies for each copy using XOR operation and insert fingerprints in individual documents. The collaboration of XOR operation and custom policies archives higher security from internal as well as external attacks. On the other hand, the data recovery approach has been designed to extract a fingerprint from secure copies. In the extensive experimental analysis, we evaluate proposed results with numerous existing systems and show the effectiveness of proposed modules in a distributed environment.

Key Words : *data security, data privacy, distribution of data, data leakage, privacy preservation, fingerprint insertion, removal .*

I. INTRODUCTION

As an appealing upcoming networking standard, the Internet of Things (IoT) connects billions of optical viewfinders, intelligent nodes, people, applications, and other physical items to provide an easy information linkage, interaction, and exchange. The application of devices and cognitive services available in the IoT is rapidly expanding due to the enormous industrial and corporate potential that exists only within IoT. The Internet of Things (IoT) has permeated much quality of the natural world. Recent, thanks to rapidly developing infrastructure and application support, to actualize various applications such as E-healthcare systems (EHSs), Internet of Vehicles (IoV), and portable crowdsensing systems. Almost every type of data about humanity and the physical universe can be gathered, distributed, and

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1989 – 2002
integrated into these diverse IoT-based technologies. The valuable information included in these data types can then be retrieved using advanced business applications, analyzing, and mining techniques to enable intelligent and omnipresent services. Security threats, such as privacy preservation, secure data storage, exchanging, and analysis, are now becoming significant hurdles for these IoT applications when more and more mortal data has been processed in current IoT-based implementations and the considerable financial returns behind privacy-sensitive and patent-sensitive data. Furthermore, In Bloom, a university digital storage company, shut down in 2014 due to public concern over the privacy protection of students' data, even though there was no evidence that In Bloom utilized students' data improperly. As a result, it is increasingly essential for SPs to protect private data from being exposed while meeting functional needs and ensuring the service quality of IoT-based apps. Because these activities offer potential dangers to privacy, providing security protocols to data transfer and examination procedures among SPs and network administrators plays a significant role in achieving this goal. SPs should integrate machine learning and mining methods that are capable of respecting privacy.

Furthermore, to accomplish a secure data exchange from data owners to SPs, secure trading and proper data taxation policies are required. Furthermore, procedures to incentivize data owners should be established to encourage them to disclose their data honestly. In light of the following issues, this essay focuses on three critical issues in research methodology, trading, and aggregation, as well as research privacy-preserving strategies and processes in the IoT.

II. LITERATURE SURVEY

A. Existing Methodologies

In A distributed analytics platform for IoT devices that avoids raw data transmission to save latency. The distributed architecture uses all participants' computational resources for the optimal global solution, such as edge devices and fog nodes [1]. A cryptographic-based privacy-preserving approach is proposed to protect data holders' privacy better. Security research showed that an honest but curious neighbour could not infer private information about any edge device's raw data. Moreover, unlike the proposed distributed approach without encryption, the safe protocol's output stays accurate. We also tested seismic imaging, diabetes progression prediction, and Enron email classification. As for seismic imaging, the proposed technique may be up to an order of magnitude faster than the standards. The assessment's results validate the methodology's effectiveness and demonstrate its viability as a data analytics solution for fog-enabled IoT devices.

Various big data analytics may assess user behaviour, resulting in privacy breaches [2]. Consequently, this article emphasizes dangers and security issues that emerge throughout the life cycle of big data by validating current standards and analyzing relevant research. We also established a security taxonomy for the big data life cycle based on the identified risks and security issues. Anonymization, aggregation, and pseudonymization are all privacy-protecting techniques that Stallings et al. [3] discussed in depth. This article examines whether these technological safeguards are sufficiently specified and effective. Before diving

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1989 – 2002
into technical protection, it's essential to grasp the breadth of action. The customer, the business, and the meaning of personal information are all vital. A privacy-preserving auction system that allows data providers to sell data securely using OTP and homomorphic encryption. They fixed altered messages and evil entities. The additional signature verification method increased processing time. However, they offered various solutions. Xu et al. [5] proposed CP-ABE, citing current IoT Cloud attribute-based encryption constraints. It addressed issues like legitimate access after user revocation and transient decryption key exposure in IoT cloud environments.

Al-Odat et al. [6] suggested SHA-based distributed ample data storage. Thus, even if part of the encryption key is acquired via Shamir0s secret sharing, data cannot be decrypted.

Greene et al. [7] said that the GDPR makes it difficult for many businesses and researchers to comply with laws and gather data. They also discuss how GDPR may affect the job of data scientists and researchers. Gahar et al. [8] studied the impact of missing data on current statistical algorithms' performance. They suggested a reduction method based on the RHadoop MapReduce paradigm to address the missing data issue. They utilized a random forest imputation technique for dispersed statistics. The method uses PCA and MCA. PCA analyses numerical data, whereas MCA processes categorical data. It also improves data search by decreasing the search space required to retrieve relevant data. Blockchain to Preserve Privacy in Resource-Constrained IoT Devices: A Survey [9] Discuss IoT applications in different fields, as well as privacy issues with resource-constrained devices. We look at how blockchain is being used in various industries and how it may help solve IoT privacy issues. Then we review further research on blockchain in IoT. This post will cover current research on IoT privacy protection using blockchain. We found that the blockchain is the best technique for preventing identity disclosure, monitoring, and tracking in IoT.

Blockchain has gained in popularity since its usage in bitcoin [10]. Blockchain is being utilized in education, healthcare, finance, agriculture, and other fields due to its advantages. One of the key features of blockchain is decentralization. It is also used as a consensus mechanism in decentralized networks like Bitcoin and Ethereum. Decentralized IoT devices may benefit from blockchain technology.

The Internet of Things (IoT) is a system that links a large number of individually identifiable items, such as computers, smartphones, sensors, software, cars, vending machines, thermostats, and other devices, to analyze and share data without the need for human intervention. It is dependent on the Internet for communication across different devices to keep the data synchronized [11]. The apparatus may be remotely controlled to do the necessary tasks.

In [12], Serena et al. proposed a privacy-preserving approach in a multi-IoT system that prevents feature disclosure. The process is based on the notions of t-closeness and k-anonymity from database theory. In these two ideas, the resilience of a group is derived from privacy requirements. It forbids the exposing of characteristics as well as the disclosure of information. Their approach also protects against the disruptive effects of malicious object

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1989 – 2002
analysis. The primary topic is multi-network representation, which is reliant on each recognized group's network link. Nodes may be used to represent any object. Inner arcs are group connections that are the same amongst entities inside the present communication network, while cross arcs are distinct group interactions. An IoT-Based Anonymous Function for Security and Privacy in Healthcare Sensor Networks [13] presents a method for anonymizing sensitive health data transmitted through wireless communication in an IoT context. The algorithm defines records that cannot be disclosed during the data session, ensuring user privacy. The proposed method also incorporates a safe encryption technique to protect patient data. We also tested the algorithm's anonymity function mathematically. The findings indicate that when used in healthcare communication networks, anonymization enhances the IoT system's security. LBS Privacy Protection in Mobile Social Networks [14]. First, consider the dynamic and global connection between k-anonymity and l-diversity. In order to improve cooperative user efficiency in LBS queries, a service category table-based method (SCTB) is developed. Finally, we utilise theoretical performance analysis and comprehensive practical studies to validate our SCTB technique. Location-based services (LBS) have grown more popular as mobile communication technology and smartphones have advanced. Users may ask location-based service providers (LBSP) for customised services based on their location, for as locating the closest restaurant, a tour guide, or a local market.

Another Way to Protect Location Privacy [15]. Then we will offer a blockchain-based location privacy protection approach. Our approach uses k-anonymity to preserve privacy and does not need third-party anonymizing services. Using several private blockchains to distribute user transaction data may enhance location privacy while maintaining service quality. We suggest an incentive scheme to promote participation. Finally, we demonstrate our method on the Remix blockchain, highlighting potential distributed network applications. location-based privacy protection We use several private blockchains to protect your location without a third party. Then we utilise distant blockchain nodes to deactivate the user-LSP connection. Anonymous LBS servers and other attackers cannot access the user's location data. The k-anonymity concept is used to protect users' privacy while delivering precise location services.

Access Control for IoT Systems and Blockchain Platforms [16]. Examining the various IoT access control methods. A table comparing the studied access control methods A comparison of methods is made in scalability and policy enforcement. We also offer categories. Decentralized access control for IoT systems: problems and potential research areas The Internet of Things (IoT) is a network of digital things. IoT improves our lives in many areas, including health, smart cities, transportation, and Smart Grids. Access control for IoT was divided into two categories using IoT paradigms and the blockchain concept: centralized and decentralized access control, with subclasses for each. There is a table that compares the different techniques of access control stated. Furthermore, conventional access control techniques for IoT devices are now controlled by a centralized authority, resulting in a single point of failure or privacy violations.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1989 – 2002
In 5G IoT, Deep Reinforcement Learning is used. UbiPriSEQ is an acronym for HetNets that manage privacy, security, energy, and quality of service [17]. Deep Reinforcement Learning (DRL) is utilized in the UbiPriSEQ framework to enhance quality of service, energy efficiency, security, and privacy in a flexible, dynamic, and holistic manner. UbiPriSEQ is a two-module system with a three-tiered design. UbiPriSEQ develops policies and decisions on critical variables like data and computation offloading rates, radio channel statuses, transmit power, task priority, and fog node selection for offloading and data migration. UbiPriSEQ is built in Python and is powered by the TensorFlow framework. It has been tested in a real-world application for SINR, privacy metric, latency, and utility function, and it shows great promise. Cyber-physical systems include, for example, smart cities and civilizations (CPSs).

Trust Hardware-Based Secure Privacy-Preserving Computation Systems for Three-Dimensional Data [18]. A privacy-preserving computing system (SPPCS) distributed file store, trusted execution environment (TEE), and blockchain technology is used for sensitive data protection. The SPPCS separates storage and analytical computations from consensus to offer a hierarchical computing architecture. The SPPCS finds data that need matching lists based on graph structure similarity calculations to avoid erroneous transactions. The SPPCS employs TEE technology to build a dual hybrid isolation architecture that restricts raw data access while concealing relationships between transaction participants [19] [20].

A Blockchain-based mobile crowdsourcing technique that protects privacy [21]. BPCM is a blockchain-based crowdsourcing method that protects mobile privacy. Blockchain-based mobile crowdsourcing protects both participants' privacy and the integrity of service requests and delivery. Then DBSCAN and IDP are used to cluster the requestors and build service strategies. Simple additive weighting (SAW) and multiple criteria decision making (MCDM) is also used to optimize service time, revenue, and provider energy consumption. Finally, rigorous testing ensures BPCM's accuracy and effectiveness.

The Dynamic Internet of Things (IoT) and Privacy [22]. Ideas, techniques, and algorithms of different distributed computing paradigms To provide a collaborative decision-making framework for heterogeneous entities in a distributed environment, this research will focus on IoT privacy issues. We also utilize the Dempster-Shafer evidence theory to demonstrate our privacy-preserving trust model. In the future, this technology may allow collaborative environments such as the Internet of Things to maintain anonymity and nonrepudiation.

Over Lattices, Privacy-Preserving Data Sharing for Secure Cloud Storage [23] A data-sharing system across lattice may be established by creating effective identity-based broadcast encryption (IBBE) technique. Except for the data owner, no one knows who the authorized data recipients are. The suggested IBBE technique protects data against selective identification and chosen-ciphertext assaults (IND-sID-CCA). It is demonstrated that the random oracle model security is based on the difficulty of learning with errors, which may resist quantum attacks. The proposed data-sharing system has several advantages over the planned IBBE method. The size of all public parameters, private keys, and ciphertexts stay consistent for all data recipients in the proposed system.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1989 – 2002
As a consequence, the proposed system can cater to a wide range of receivers. The proposed data-sharing mechanism also promotes membership. In this case, the present recipient does not need to update their private key. Decryption costs will not change when outsourced data is updated.

Distributed Incentive-Based Monitoring for VANET Traffic Security [24]. A distributed trust management system based on the Byzantine fault-tolerant Paxos algorithm and game theory Unlike current models, the suggested method can check the accuracy of broadcast information when hostile automobiles outnumber non-malicious vehicles. A non-malicious vehicle at each RSU was utilized to test the proposed system's practicality and effectiveness.

For efficient key-aggregate keyword searchable encryption, [25] suggested an EVKAKSE. Users may establish a single gateway for keyword search across shared files using the aggregate key provided by the data owner. We explain the scheme's requirements, threat models, and design. Our security study and experimental evaluation also demonstrate the scheme's efficiency and security.

Security and privacy in vehicular networks using Blockchain [26]. A privacy-preserving trust management system that utilizes blockchain to evaluate vehicle reliability. We build a blockchain-based trust evaluation system that uses ratings from adjacent vehicles to determine a vehicle's trustworthiness. We develop feedback message aggregation and trust assessment on two intelligent contracts to enable fast and privacy-preserving trust evaluation. Vehicle privacy is protected using the Elliptic Curve Cryptography (ECC) cryptosystem. According to security and performance tests, our system is secure and efficient in handling trust evaluation for vehicle networks.

Huang et al. [27] proposed a novel cloud-based approach for data exchange between users and regulated dissemination for different owners. Identity-based Broadcast Encryption (IBBE) is used to transmit data between users. The owners also define a fine-grained access structure based on preferences. The proposed approach provides adequate data security in multi-owner clouds.

How to include privacy protection in blockchain-based IoT systems [28]. We can solve privacy issues highlighted by blockchain in IoT applications by focusing on the apps we use every day. Anonymization, encryption, private contracts, mixing, and differential privacy is five privacy-preserving methods in blockchain-based IoT systems. Finally, we discuss the challenges and future of blockchain-based IoT privacy research. For future IoT systems that utilize the blockchain to address privacy problems, this article may be helpful. Improved Honeypot cryptographic technique for cloud security prediction [29]. Data must be protected against infiltration or other kinds of attack. This technique of privacy protection uses a cryptographic mechanism. Encryption is done using the Honeypot algorithm. When a data owner requests a file, the cloud server generates a key and verifies it with the user. When the user gives the key, the file is decrypted and delivered to the user. Finally, a performance analysis is performed, along with comparing existing and new techniques to show the

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1989 – 2002
suggested scheme's effectiveness. Privacy conflicts while outsourcing computation to ECDs in IoV still exist [30].

III. PROPOSED SYSTEM DESIGN

The below figure 1 describes the proposed system architecture with strategic execution. Initially, we collect synthetic and natural time data from various sources such as IoT resources, historical data, and runtime data collection from various web applications. In such a data could be e contains sensitive information of users. Moreover, it is required to generate a privacy view during the date of broadcasting. This research defines some security policies in a pre-trained model, and it's applied to data distribution. The privacy view works like the Data Hiding technique, which eliminates database attacks and privacy breaching issues

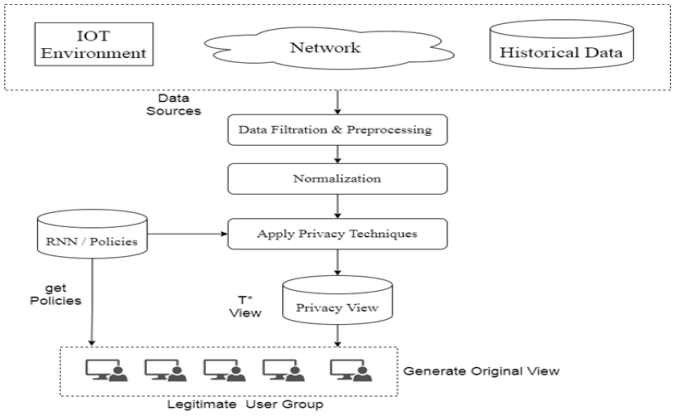

Fig. 1 Proposed system architecture

Secure multiparty computation (SMC) protocol is another technique used to achieve the privacy enlarge synthetic data when broadcasting [10]. In our research, we applied XOR and function for generator fingerprint for multiple copies. Each copy contains minimum fingerprint values, which provide security to those documents and easy to identify traitor by analysis the malicious copies.

IV. ALGORITHM DESIGN

This section describes about both privacy and fingerprint generation algorithm, on large input data matrix to generate the number of secret copies. Algorithm 1 ensures avoid data breaches and eliminate the internal and external collusion attacks. In order to achieve verification of actual data fingerprint removal algorithm need to write for detection of attackers in case of validation of data leakage or unauthorized user.

A: Algorithm for secure fingerprinted copy generation

Input: Dataset Data[], privacy policies {p1,p2,p3…..pn}, XOR operation, Number of fingerprinted copies n, secret key K.

Output: n secure data copies [T1……Tn]

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1989 – 2002
Step 1 : Read data from dataset using below function and add into data matrix

$$Collection\_Col\_Row\ [] = \sum_{n=0}^{\infty} (Data_{[n]}\ .\ column[0] \dots column[max]) \quad \text{…..eq. (1)}$$

Step 2 : Read add privacy policies from dictionary using below function

$$Collection\_pol\ [] = \sum_{n=0}^{\infty} (att[0] \dots att[max]) \quad \text{…..eq. (2)}$$

Step 3: Select the number of copies as n for distribution

Step 4 : Foreach (k into n)

$$Val = (int) \sum_{n=1}^{\infty} (Log10\ (Random * K)) \quad \text{…..eq. (3)}$$

Step 5 : Generate fingerprinted copy T*

T* ← XOR (**Error! Reference source not found.** ,K)

T*[] ← add(T*) …..eq. (4)

Step 6: Return T[]*

This method is similar to one-way hash functions in how it generates the privacy view. The goal of this method is to keep sensitive data secure and avoid privacy intrusions. As a result, anonymous views on miniature buckets are generated.

B: Algorithm for privacy view generation

Input: Input dataset DSet, total number of data providers Dp, Constraint policy C {K_Anonimity, L_Diversity}

Output: Privacy view (NT*) with selective provider

Step 1: foreach (DSet till null)

Step 2: foreach (col in table)

foreach (row in table)

Step 3: Select quasi identifier (QiF) and set of sensitive attributes (S_Att)

Step 4: Executes generalization to classify the tupples in QiF with multiple groups

Step 5: Perform anonymization on entire set of attributes

Step 6: While **(**validate data privacy(DSet, Dp, C) = 0) do

if (DSet[i] ← DSet) validated with QiF then

add D[i] till K-anonimity

else break;

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1989 – 2002
Bucket_List(i1) DSet;

Step 7: Apply permutation on dataset (DSet[i]=(I(null-1)))

Step 8: Apply Pruning on(DSet)

Step 9: Execute step 1,2,3 on Bucket_List (i1)

Step 10: if (C != (DSet) && (Dp # 1))

Bucket(i2) Bucket_List (i1(j))

Step 11: Show (Bucket_List (i2)!=null)

Step 12: end while end for

The top-down and bottom-up algorithm is similar to the base-up method. The main difference is in how coalition checks are performed, starting with 0-foe and working up. When an infringement by any foe is detected (early stop) or all m-policies are examined, the algorithm comes to a cessation. The algorithm represents the basic idea of a bottom-up speculating approach.

C: Algorithm Top down and Bottom up generalization view

Step 1 : Read data from dataset from bottom set or top set

$$data[] = \sum_{n=1}^{m} (\text{Row } [n]) \qquad \text{.....eq. (5)}$$

Step 2: Check data count with K-anonimity ad L-diversity for each block

Step 3: calculate the fitness score F_Score(DataSet[])

Step 4 : if (F_Score >= Th)

Generate best generalized view as T*

Step 5 : end loop

Step 6: return T*;

V. RESULTS AND DISCUSSIONS

In A The proposed system has carried out various data set for experiment analysis. Four different data set has been used to execute the proposed approach. Clinical GD health care dataset set has taken from US government Healthcare website, the heart data set has taken from IoT heart device, and diabetic datasheet has taken from weka tool respectively.

Classification of data with different numbers of data size, number of fold validations as well as different classification algorithms. This section describes the privacy scenario of proposed

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1989 – 2002
system how it communicates with end use using Graphical User Interface (GUI). Basically, many privacy algorithms, have been proposed in existing systems like Generalization, Anonimzation, Random Permutation, slicing, Bucketization etc. In work carried out SHA based privacy approach as well as key based privacy approach during data distribution. System also follow Secure Multiparty Computation (SMC) for to achieved the highest security. In the existing privacy techniques having some data leakage issue which generate data losses during the distribution. One way Hash Function based security techniques also described in existing approaches but such a system but it generates high time as well as space complexity. The privacy technique basically illustrates how to hide sensitive information of specific attribute. Sensitive Attribute (SA) and Quasi Identifier (QI) are the important set-in privacy distribution. Some systems also described if score calculation of specific set. Slicing techniques have been proposed with random permutation and bucketization. The proposed system describes key based hash function as well as SHA-256 family function.

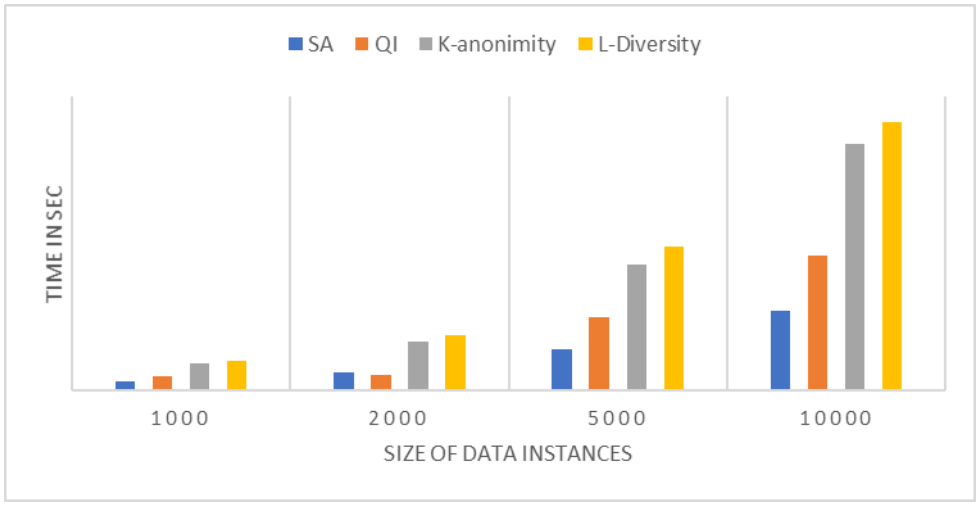

Fig. 2 Data privacy view generation computation with different functions

The above figure 2 describes data distribution time complexity for different records set, four techniques has used to on different attributes like SA, QI, K-Anonimity and L-Diversity respectively. The time has measure in various experimental analyses; time describes in milliseconds shows for all instances.

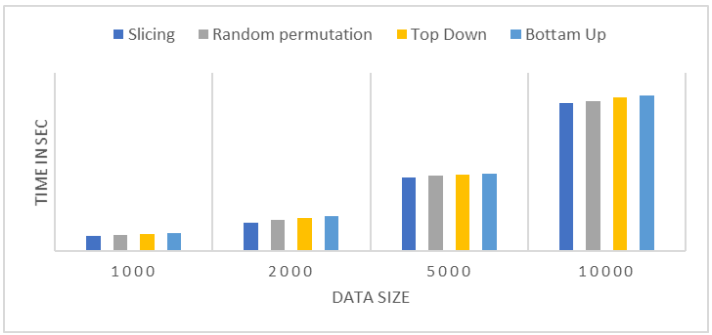

Fig. 3 Data distribution time complexity with different functions

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1989 – 2002
This figure 3 shows the data distribution time complexity for slicing, Random Permutation, Top-down approach and Bottom-up generalization respectively. System test data consist around 25000 instances; various experiments are generated for secure data distribution. The above also shows time required in milliseconds for data distribution as well as x axis shows the number of instances has given input to respective process.

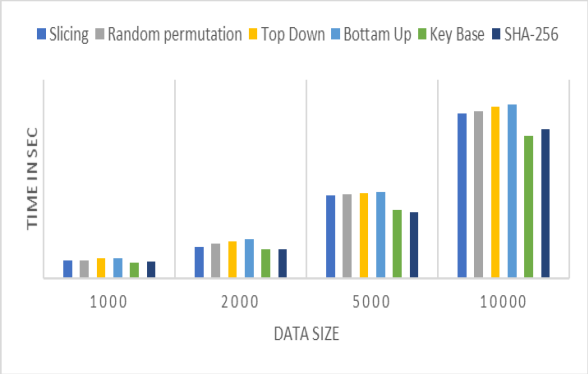

Fig. 4 Data distribution time complexity with different functions

The above figure 4 shows the privacy base time comparative analysis of system, four existing techniques have been used to evaluate with proposed system. Existing strategies have been evaluated the performance analysis of system, in existing systems Slicing, Random Permutation, Top-Down Generalization as well as bottom of generalization approach have been proposed with secure multiparty computation protocol. The F-Score has been used for verification of specific instances in various privacy techniques, some approaches carried out provider aware privacy algorithms for security distribution. The basic drawbacks of existing privacy preservation approach they follow some pruning strategies during the verification or data distribution, such protocols might be generates high time complexity. In top down and bottom-up generalization system use third party server for user authentication in peer-to-peer network, it is most secure method for data distribution in privacy techniques. The basic drawback of these system which generates third party resources dependency during the peer verification, in case if third party server not available, when system broadcast the data then it generates data inconsistency or data unavailability, which occurs the problem of data leakage or data reduction. To eliminate the such tribulations in propose work system focus on SHA-256 hashing technique as well as Key based Hash Function for Secure data distribution. That is data consists some quasi identifier as well as some sensitive attributes.

The proposed functions overall accuracy is better than all existing approaches, patient dataset consist multiple Sensitive Attribute (SA) like all health attributes and must require privacy during the data distribution

VI. CONCLUSION AND FUTURE WORK

Maintaining privacy during the data of distribution was another perspective behind this research; we have studied some existing privacy and security-based techniques like data Anonymization, generalization, random permutation, slicing, bucketization etc. The current

privacy techniques illustrate the one-way privacy technique, which works like a secure multiparty computation protocol. These existing techniques also generate high time complexity. To overcome such issues, designed numerous privacy-based algorithms and hash-based privacy. The proposed privacy techniques also work like one-way hash functions, but both operations carried out customized byte code generation techniques, which significantly reduces the privacy has size during the data distribution. In future work to enhance the system with fingerprint extraction for all n copies and trace the data consistency with proposed security tuning protocols.

ACKNOWLEDGMENTS

I would like to express my deep gratitude to Research Dean, Head of Department of Computer Science and Engineering, my research supervisor valuable guidance for providing required resources to carry out research work. I would also like to thank Honorable Managing Trustee of Sanjivani College of Engineering, Kopargaon, India, Head of Department of Information Technology for providing support for the research work.

REFERENCES

1. Rohit Ravindra Nikam, Rekha Shahapurkar, “Data Privacy Preservation and Security Approaches for Sensitive Data in Big Data”, 2021 The authors and IOS Press doi:10.3233/APC210221 page 394-408.
2. Zhao, Liang. "Privacy-Preserving Distributed Analytics in Fog-Enabled IoT Systems." Sensors 20.21 (2020): 6153.
3. Koo, Jahoon, Giluk Kang, and Young-Gab Kim. "Security and Privacy in Big Data Life Cycle: A Survey and Open Challenges." Sustainability 12.24 (2020): 10571.
4. Stallings, W. Handling of Personal Information and Deidentified, Aggregated, and Pseudonymized Information under the California Consumer Privacy Act. IEEE Secur. Priv. 2020, 18, 61–64. [CrossRef]
5. Gao, W.; Yu, W.; Liang, F.; Hatcher, W.G.; Lu, C. Privacy-preserving auction for big data trading using homomorphic encryption. IEEE Trans. Netw. Sci. Eng. 2020, 7, 776–791. [CrossRef]
6. Xu, S.; Yang, G.; Mu, Y.; Liu, X. A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance. Future Gener. Comput. Syst. 2019, 97, 284–294. [CrossRef]
7. Al-Odat, Z.; Al-Qtiemat, E.; Khan, S. A big data storage scheme based on distributed storage locations and multiple authorizations. In Proceedings of the 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS),Washington, DC, USA, 27–29 May 2019. [CrossRef]
8. Greene, T.; Shmueli, G.; Ray, S.; Fell, J. Adjusting to the GDPR: The impact on data scientists and behavioral researchers. Big Data 2019, 7, 140–162.
9. Gahar, R.M.; Arfaoui, O.; Hidri, M.S.; Hadj-Alouane, N.B. A Distributed Approach for High-Dimensionality Heterogeneous Data Reduction. IEEE Access 2019, 7, 151006–151022.

10. Iftikhar, Zainab, et al. "Privacy Preservation in Resource-Constrained IoT Devices Using Blockchain—A Survey." Electronics 10.14 (2021): 1732.
11. Nakamoto, S.; Bitcoin, A. A Peer-To-Peer Electronic Cash System. Bitcoin. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 12 October 2020).
12. Elijah, O.; Rahman, T.; Orikumhi, I.; Leow, C.; Hindia, M. An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. IEEE Internet Things J. 2018, 5, 3758–3773. [CrossRef]
13. Yin, Xiao Chun, et al. "An IoT-based anonymous function for security and privacy in healthcare sensor networks." Sensors 19.14 (2019): 3146.
14. Yang, Guangcan, et al. "An efficient approach for LBS privacy preservation in mobile social networks." Applied Sciences 9.2 (2019): 316.
15. Qiu, Ying, et al. "A novel location privacy-preserving approach based on blockchain." Sensors 20.12 (2020): 3519.
16. Abdi, Adam Ibrahim, et al. "Blockchain Platforms and Access Control Classification for IoT Systems." Symmetry 12.10 (2020): 1663.
17. Mohammed, Thaha, et al. "UbiPriSEQ—Deep reinforcement learning to manage privacy, security, energy, and QoS in 5G IoT hetnets." Applied Sciences 10.20 (2020): 7120.
18. Yuan, Munan, et al. "Trust Hardware Based Secured Privacy Preserving Computation System for Three-Dimensional Data." Electronics 10.13 (2021): 1546.
19. Firdaus, Muhammad, and Kyung-Hyune Rhee. "On blockchain-enhanced secure data storage and sharing in vehicular edge computing networks." Applied Sciences 11.1 (2021): 414.
20. Tan, Shengmin, Xu Wang, and Chuanwen Jiang. "Privacy-preserving energy scheduling for ESCOs based on energy blockchain network." Energies 12.8 (2019): 1530.
21. Xu, Xiaolong, et al. "A blockchain-powered crowdsourcing method with privacy preservation in mobile environment." IEEE Transactions on Computational Social Systems 6.6 (2019): 1407-1419.
22. MacDermott, Áine, et al. "Privacy preserving issues in the dynamic internet of things (IoT)." 2020 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2020.
23. Wang, Fenghe, Junquan Wang, and Shaoquan Shi. "Efficient Data Sharing With Privacy Preservation Over Lattices for Secure Cloud Storage." IEEE Systems Journal (2021).
24. Roy, Ayan, and Sanjay Madria. "Distributed Incentive-Based Secured Traffic Monitoring in VANETs." 2020 21st IEEE International Conference on Mobile Data Management (MDM). IEEE, 2020.
25. Wang, Xuqi, Xiangguo Cheng, and Yu Xie. "Efficient verifiable key-aggregate keyword searchable encryption for data sharing in outsourcing storage." IEEE Access 8 (2019): 11732-11742.
26. Wang, Danxin, et al. "A Privacy-Preserving Trust Management System based on Blockchain for Vehicular Networks." 2021 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2021.

27. Miao, Y.; Liu, X.; Choo, K.-K.R.; Deng, R.H.; Li, J.; Li, H.; Ma, J. Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-owner Setting. IEEE Trans. Dependable Secur. Comput. 2019, 1.
28. Hassan, Muneeb Ul, Mubashir Husain Rehmani, and Jinjun Chen. "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions." Future Generation Computer Systems 97 (2019): 512-529.
29. Mondal, Avijit, and Radha Tamal Goswami. "Enhanced Honeypot cryptographic scheme and privacy preservation for an effective prediction in cloud security." Microprocessors and Microsystems 81 (2021): 103719.
30. Xu, Xiaolong, et al. "An edge computing-enabled computation offloading method with privacy preservation for internet of connected vehicles." Future Gen ration Computer Systems 96 (2019): 89-100.