# Scalable Data Partitioning Strategies for Hybrid Cloud Environments

Rajendra Baleshwar[1], Ramesh Vishwakarma[2]
[1,2]*Department of Computer Science, Rabindranath Tagore University, Bhopal (M.P.)*

***Abstract:*** **When it comes to storage and analytics, private clouds are preferred by enterprises that deal with very sensitive data. Due to the fact that private cloud is designed for usage by a single business, the danger to the organization's security and privacy is significantly reduced. Despite this, private cloud computing does have some restrictions when it comes to the processing of data. The scalability concern is the first limitation that must be considered. The private cloud that is run on-premises does not take into consideration the flood of data, and as a result, it has limited scalability. For the purpose of constructing private clouds that are highly scalable, it is necessary to make a substantial initial expenditure with the intention of acquiring and installing computing resources. When it comes to precisely planning the storage limit of a private cloud, however, the dynamic properties of big data, such as increasing volume, velocity, and diversity, result in issues. As a consequence of this, the capacity of private clouds is perpetually either fully or partially provided. Developing a private cloud that has restricted scalability is being done primarily for the purpose of lowering the amount of money that is being invested in its creation. For the purpose of storing and processing large amounts of data, many cloud computing models, including private cloud, public cloud, and hybrid cloud, are utilized, depending on the requirements.**

**Keyword: Private cloud, Public cloud, Hybrid cloud, Big data**

## I. INTRODUCTION

The perspective of cloud computing, a cloud infrastructure is made up of two or more clouds (private, communal, or public) that operate independently of one another but are connected to one another by proprietary or standard protocols that allow for the creation of data. A further possibility is that programs may move around (for example, cloud bursting technology makes it possible to share load across many clouds). When customers use this method, they often choose to outsource data processing that is not considered to be enterprise-critical to the public cloud. At the same time, they continue to have power over the most important data and services that the company provides. The capabilities of public clouds and private clouds are combined in hybrid clouds via the use of technologies that make it easier for data and applications to move between the two types of clouds. The hybrid cloud provides businesses with a broader number of deployment choices as well as more flexibility, which is beneficial to the businesses. This is done in order to facilitate the transfer of data and programs between private and public clouds, which is made possible by hybrid clouds.

The rise of big data and the growing popularity of big data analytics will inevitably result in the requirement for storage and processing frameworks that are hosted on the cloud. This enormous volume of data is kept on the cloud, where it is also successfully shared among users who have been permitted to access it. It is necessary to have security and privacy methods in place in order to guarantee the integrity of data that is kept in the cloud since once data is moved to the cloud, the owner of the data no longer has direct control over the data. The large dataset that is stored in the cloud is vulnerable to assaults, whether they are purposeful or unintentional, as well as hardware breakdowns. As a result, ensuring the safety of data stored in the cloud is an unavoidable necessity and the most important problem to resolve. Since the disclosure of sensitive or private data stored in the cloud might result in significant harm to the owner of the data, it is imperative that this data be safeguarded at all costs. All of the many deployment options of cloud computing, including public, private, and hybrid cloud, have a significant worry regarding the security of cloud storage. According to Wei et al.'s [2015] description, the ever-evolving big-data standard has had a significant impact on our society, and it will continue to captivate a variety of perspectives from both technical experts and the general people. This is

because of the wide influence that it has had. In recent times, the big data model has been recognized for its substantial responsiveness. This is due to the fact that it offers a vast opportunity to extract patterns from massive amounts of data.

The capabilities that are gained via the use of a network are referred to as services in the cloud computing technology of today. Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a Service (SaaS) are the facets of cloud computing that have shown to be the most advantageous, as stated by Tan et al., [2014]. The amount, pace, diversity, authenticity, and usefulness of data that is being produced across a range of disciplines are evolving at an astounding rate, and we are experiencing this development. One of the distinguishing features of big data is that it requires the utilization of cloud computing for both storage and processing purposes respectively. The concept of cloud computing is receiving a lot of attention as one of the most significant advancements in information technology in the modern era. Therefore, cloud computing has become the technology of choice for data analytics since it offers a vast array of resources as services and charges users depending on their consumption patterns. This is accomplished through the utilization of the resource virtualization idea. It is usual for cloud computing to be associated with security and privacy risks, and as a result, there is reluctance to use cloud computing. As soon as data is sent to the cloud, the owner of the data loses control over their data, which is in direct opposition to the conventional data processing methods. When it comes to storing sensitive data on the cloud, the most difficult issue is figuring out the methods that are required to guarantee both confidentiality and integrity.

## II REVIEW OF THE LITEATURE

In Strohbach et al., (2016), the authors discussed the challenges and issues in storing colossal datasets in a "secured"and "privacy-preserved"manner. The work highlighted the salient features on an ideal big data storage system like the ability to store any amount and nature (homogenous and heterogeneous) of data, effective retrieval and searching mechanisms, fault tolerance, optimal data transfers, security and privacy of data etc. They also gave the overview of the "social"and "economic"implications of big data "storage-technologies"on the basis of case studies ranging from healthcare, finance and energy sectors. The work dives deep into discussing big data storage technologies, big data query platforms like "HBase", "HIVE", and "Impala"etc. Finally, the work puts forward some of the best practices for implementing security features in big data management systems and was concluded by highlighting the requirements for effective and efficient storage of huge datasets.

In Park and Kim (2018), the authors introduced a new prototype "large capacity storage device"using the "network direct connection storage"device in order to effectively store and process big data. The work began with a description of bottlenecks in big data storage tools and infrastructures. The prime focus was on the network and storage performances. In their proposed prototype, there was no CPU or memory provided at the network side. The storage and I/O were handled by self-designed protocol suite itself using protocol for the exchange of data and thus no network stack was present in their approach. They performed the empirical evaluation for validating the performance and scalability enhancement of their proposal. Finally, they concluded that the performance of their system is directly proportional to the number of disks in the device. The more the number of disks, the better is the performance. However, they did not mention about the security measures taken to ensure the security of the stored big data. Without security mechanisms, the storage of data involves high risks and thus their approach cannot be applicable in general big data storage systems which require secured storage of data.

The authors in Zhou et al.,(2018) proposed and implemented a novel "Preference Aware HDFS (PAHDFS)"system with an aim to improve the performance of classical Hadoop system in hybrid environments. The primary concern addressed in their work was the imbalance of storage and its effects on the performance of the system when the data is stored in a distributed manner. They first described the properties of "Hard Disk Drives (HDDs)"and "Solid State Drives (SSDs)". The limitations of Hadoop that it considered all storage devices having the same I/O throughput and distributes the data across all clusters in an even manner were highlighted. They also mentioned that a distributed system may have multiple kinds of storage devices and each of these devices largely differ in the format, capacity and capabilities of handling data. Thus it is necessary to store the data

in the most appropriate storage device in order to achieve optimal performance. The proposed model works by tracking the read/write characteristics of the data and optimally chooses the most suitable device in accordance with the matching read/write capacities of the device thereby increasing the read/write efficiency.

The authors in Li et al., (2017) discussed about a novel cryptographic approach for securing the big data. The authors highlighted the importance of securing the data stored on the cloud and the user's apprehensions against the adoption of cloud computing. The data stored on clouds are always prone to illegitimate access and thefts. There are several state of the art techniques already in place for securing the data on the cloud but still the end user is apprehended from adopting the cloud technology with confidence. With this apprehension as a motivation, their work provides a cryptographic technique to obscure the contents of the data stored on the cloud. The work proceeded with introduction of cloud computing environment and its advantages and limitations along with the examples of major enterprises using the cloud computing approach for data management purposes. The approach works by dividing the files into various categories and stores the parts distinctly along with the identification of files which needs splitting. They named their approach as "Security-Aware Efficient Distributed Storage (SA-EDS)"and the underlying algorithms were called as "Alternative Data Distribution (AD2)"algorithm, "Secure Efficient Data Distributions (SED2)"algorithm and "Efficient Data Conflation (EDCon)"algorithm. The architecture follows a simple identification in which the normal data and sensitive data were separated. The normal data is stored using the conventional storage mechanism while the sensitive data is first broken into several parts and each part is stored separately on a different cloud. At the time of retrieval, the sensitive data from different clouds gets merged and then transferred to the client who requested for it. On the basis of empirical evaluations, they claim to overcome the security threats to big data in "cloud computing"environment. However, it was observed in their work that the data is getting separated into multiple parts only when it is characterized as sensitive, but the criteria of sensitivity was not defined anywhere in the proposal. Secondly, the work claims to store the normal data onto a single cloud server which is practically not possible considering the scale of production of data.

Faraway and Augustin (2018) argued that big data is not always useful as compared to small data. They provided several situations wherein small data is preferred over big data to draw much better inferences. The work started with defining big and small data and then the situations when small data can overpower big data were highlighted. The authors claimed that a well-organized small data is more useful than an unorganized big data in many cases. Secondly, the cost involved in managing (acquiring, storing, securing) big data is much higher as compared to managing small data. Thirdly the heterogeneity and uncertainty attached with big data makes it intricate to handle. However, no such problems are associated with small data. Finally, the work concluded with describing the problems and challenges associated with mining the relevant information for the huge datasets.

Wang et al., (2018a) conducted a study to investigate the "historical development", "architectural design"and "component functionalities"of big data analytics with respect to healthcare domain and proposed a roadmap for the healthcare domain for effectively adopting big data analytics in their routine functional activities in order to achieve better diagnosis and treatments. They stressed upon the need for realizing the strategic implications of big data analytics. To conduct their study they included twenty six case studies. The study provided a background of big data, its architecture and analytics. The research adopted the quantitative approach in which the authors collected several cases from the vendors and after studying and analyzing those case recommended five cases which are ready to adopt big data analytics within their systems. The work also presented the benefits of adopting big data analytics in a tabular format in terms of infrastructure, operational, maintenance, organizational, managerial and strategic parameters under medical domain.

Alharthi et al., (2017) discussed the tactics that can be adopted to overcome the barriers in big data system adoptions. They specifically focused on revamping the infrastructure, enhanced privacy, and big data analytics skill developments. To start with, they introduced big data and its brief history along with the

characteristics of big data primarily focusing on volume, variety and velocity. The various opportunities with big data were also discussed highlighting the usage of big data analytics in airlines, Walt Disney, United Parcel Group etc. A major portion of their work was dedicated to describing the barriers in big data technology adoptions. Specifically technical infrastructure, skill, heterogeneity and non-uniform structure of data, privacy and cultural barriers were discussed. Finally, state-of-art solutions were highlighted in a tabular format which concludes the work. The claims made by them were not supported by empirical evaluations rather only a theoretical description was provided by the authors. The effectiveness of big data storage system lies in the way it manages the data storage such that the read/write latencies are at a minimum along with a minimum possible response time. Since the data resides at multiple sites in a distributed manner, it is crucial to devise mechanisms to link these multiple sites in such a way that it follows CAP theorem (Consistency, Availability and Partition Tolerance). When we talk about distributed network there exist obvious bottlenecks, latencies and delays which must be handled effectively by a good distributed data storage system. The read/write efficiency is a prominent factor in the adoption of big data storage technology. This means that the systems which have better (faster) read/write capabilities are preferred among others.

## III OBJECTIVE OF THE STUDY

1. To study scalable data partitioning strategies for hybrid cloud environments
2. To offer safe cloud storage for the storage of vast amounts of big data.

## IV PROPOSED METHODOLOGY

The work that is proposed in this thesis splits data into three categories, such as sensitive data, insensitive data, and public data, in order to address the issues that are presented by existing schemes and to offer safe cloud storage for the storage of vast amounts of big data. This category is determined by the significance of the data contained in the large dataset. The protection of sensitive data is of the utmost importance since it is often regarded as the most valuable kinds of data. When it comes to the storage and processing of sensitive data, a private cloud is the preferable option. Data that is not sensitive is not as vital as data that is sensitive; yet, controlled data access is still required for insensitive data. Consequently, data is uploaded to the public cloud since it is shared with members of the organization as well as permitted outsiders. Data that is considered public is made available to anybody who requires access to it for usage.

Because the cloud is unavoidable for the storage and analysis of large amounts of data, it is vital for users of the cloud to partition large datasets into smaller datasets that are easier to manage and to store these datasets on a variety of physical servers. This will improve flexibility and dependability, as well as allow for efficient calculations to be applied in order to identify patterns. In the year 2010, Dong et al. Cloud data storage arranges the acquired information in a suitable way for analytics and knowledge extraction. For cloud storage to function well, the underlying storage infrastructure must be able to store data in a consistent and dependable manner. This is the fundamental need. It is also necessary for the storage system to be scalable in order to accommodate the substantial amount of big data. All of the data that is held in the cloud by cloud tenants is separated into three categories: sensitive data, insensitive data, and public data.

## V EXPERIMENTAL ANALYSIS

The file systems that are utilized in cloud storage offer a platform that is both scalable and safe for the management of data. The records are broken up into chunks, which may then be disseminated among the block servers. Additionally, the metadata server offers centralized control of the systems that are made up of interconnected groups of block servers. The ability to store and handle massive amounts of big data is made possible by this characteristic of cloud storage providers. In spite of the fact that cloud storage is effective for large amounts of data, it is of utmost importance to ensure that the data that is saved is accurate and complete. Furthermore, automated processes are required in order to detect errors and enable automatic recovery. Data may be repeatedly preserved in a large number of copies thanks to the capabilities of the file systems.

Even while traditional techniques guarantee the accuracy of data that has been outsourced without

downloading these data from cloud data stores that cannot be trusted, various algorithms are incapable of functioning properly in an environment that utilizes distributed cloud storage. The lack of homomorphism qualities in collaborative proofs, which are necessary for consumers to know the specific location of each file block in a cloud environment, is the cause of this incompetence. A consequence of this is that the authentication procedure results in substantial communication overheads as well as calculation expenses on the user's end. Therefore, it is of the utmost importance to analyze the suggested model in terms of the needed storage and network expenses, as well as to enhance the transparency of verification operations in cloud storage systems that are extendable. The model that has been proposed is examined on three different levels:

The data owner and the cloud service provider (CSP) are required to offer the data owner with alternatives for regularly confirming the integrity of sensitive data without downloading the data to client sites after the data has been uploaded to the cloud. In addition, it is necessary to keep an eye out for any instances of Service Level Agreements (SLAs) being broken in cloud storage. CSP is obligated to provide data owners with information on the storage path of partitioned data. The complexity of calculation should not be imposed on the client side with regard to data integrity verification.

Within a cloud service provider (CSP), the CSP is responsible for ensuring that the integrity of data partitions that are spread over many storage servers is checked, and problems that have been found and remedied.

It is possible to store enormous amounts of data in a distributive fashion among a number of distinct CSPs because of the large volume of big data. The necessity of frequently checking the integrity of distributed large data through cloud gate interface between cloud service providers is heightened as a result of this.

The work that is being presented is reviewed in relation to these three levels, and security is ensured for the protection of cloud data over its entire life duration.

Theoretical Analysis : During the course of this research, the computing overhead that is associated with encrypting and decrypting data is decreased by encrypting only the information about the storage path, rather than encrypting the data itself. Not only does the encrypted file index have a size of only k-bytes, but it is also relatively simple to distribute among interested parties. Under the plan that has been presented, large amounts of data will be partitioned into n pieces, and these n parts would be disseminated across m cloud service providers simultaneously.

Security Analysis: Java is used for the implementation of all of the proposed mechanisms, and the performance measurements that are taken into consideration are the price of computation, the price of bandwidth, and the assessment of storage cost. The issue of data leaking, which can lead to dangers to both integrity and privacy, is addressed in this aforementioned study. Access to the data is not available for users who are not allowed to do so. Schemes known as Proof of Retrievability (PoR) are utilized in order to guarantee the authenticity of data that is kept in the cloud. As an additional method of integrity verification, Proof of Data Possession (PDP) techniques are utilized. In this system, the servers demonstrate that the data is saved in the appropriate manner. Contrary to popular belief, the use of PRE in this work does not enable unidirectional delegation, which is a situation in which it is simple for A to delegate to B and vice versa. As a result, delegation from A to B is entirely feasible, and BA does not hold. The process of re-encryption is carried out by a proxy server; hence, it eliminates the need for a third party auditor to be involved, making it a more secure method. According to the findings of the experimental investigation that was carried out by examining the overhead of compute, communication, and storage, it produces superior outcomes. Through the utilization of hybrid cloud, storage overhead was decreased. The most significant advantage of this work is that it makes use of a private cloud for the sole purpose of storing sensitive data, which results in a reduction in overhead and ensures that security is maintained.

The metrics used for evaluating performance of encryption schemes are:

Execution Time : Time needed for executing encryption, re-encryption, and decryption operations for various parameter settings.

Throughput : Total size of plaintext that is processed (encrypted, decrypted, re-encrypted) per unit time.

Ciphertext storage : Amount of memory needed to store ciphertext for every bit of plaintext.

Memory utilization : Amount of memory needed for implementing encryption and decryption opertions.
The computation time of proposed scheme is represented in Table 1.
The encryption and decryption throughput is calculated using Equation 1.

Table 5.3: Computation Time (in ms)

| Parameter size | Encryption Time | Decryption Time | Re-Encryption Time |
|---|---|---|---|
| 512 bit | 334.82 | 337.23 | 359.11 |
| 1024 bit | 723.31 | 725.72 | 774.45 |

$$Throughput = \frac{Size\ of\ Plaintext}{Total\ Encryption\ /\ Decryption\ Time}$$

Let k be the number of bits required to represent ciphertext modulus q on plaintext modulus p and consider n as the dimension of encryption. At this setting, the execution time of encryption, decryption before re-encryption, re-encryption, and decryption after re-encryption are represented in Table 2.

Table 2: Execution Time of Proxy Re-encryption

| Setup | | | Execution Time | | | |
|---|---|---|---|---|---|---|
| n | p | k | Encryption (ms) | Decryption before Re-encryption (ms) | Re-encryption | Decryption after Re-encryption (ms) |
| 1024 | 2 | 35 | 2.13 | 2.45 | 67.08 | 2.44 |
| 2048 | 16 | 53 | 5.38 | 7.73 | 228.3 | 7.55 |
| 4096 | 256 | 78 | 16.2 | 23.05 | 516.58 | 22.98 |

With the same setting of n, p, and k values, throughput of encryption, re-encryption, and decryption after re-encryption are calculated using Equation 1 and is illustrated in Table 3.

Table 3: Throughput of Proxy Re-encryption

| Setup | | | Throughput | | |
|---|---|---|---|---|---|
| n | p | k | Encryption (Mbps) | Re-encryption (Mbps) | Decryption after Re-encryption (Mbps) |
| 1024 | 2 | 35 | 0.47 | 0.0149 | 0.409 |
| 2048 | 16 | 53 | 1.488 | 0.035 | 1.06 |
| 4096 | 256 | 78 | 1.975 | 0.315 | 1.39 |

The proposed work is compared with other approaches such as KP-ABE and CP-ABE for the measure of encryption and decryption throughput. The comparison result values are shown in Table 4. The encryption and decryption throughput of proposed method is better when compared with existing methods as shown in Figure 1.

Table 4: Throughput Comparison

| Schemes | Encryption Throughput(MB/Sec) | Decryption Throughput (MB/Sec) |
|---|---|---|
| KP-ABE | 0.52 | 0.61 |
| CP-ABE | 0.55 | 0.68 |
| Proposed | 0.67 | 0.74 |

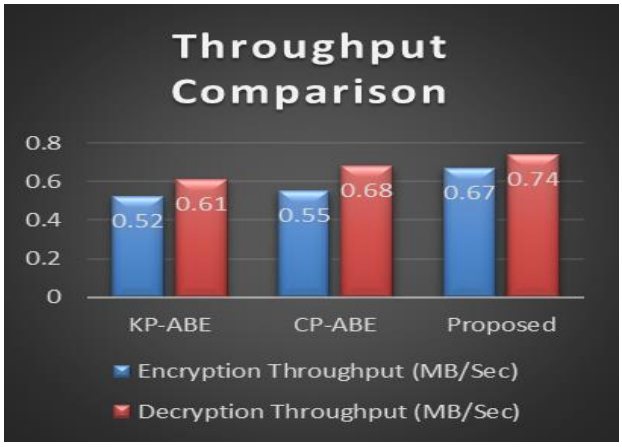


Figure 1: Encryption Vs Decryption Throughput

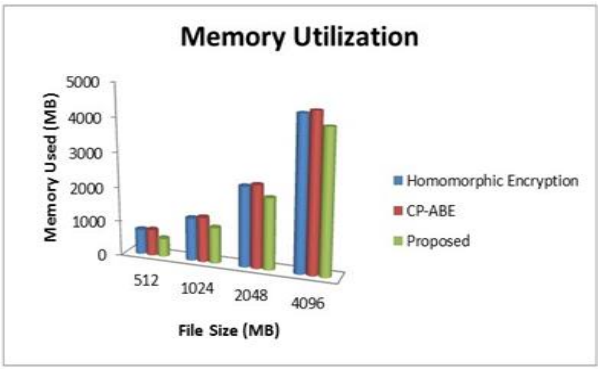


Figure 2: Memory Utilization

With the technique that has been described, both the data storage overhead and the complexity of computation are minimized. For the purpose of evaluating the amount of time required for execution, the proposed technique is

compared to homomorphic encryption and CP-ABE. It has been demonstrated that the technique that was presented requires less time to execute. Although the execution time grows in proportion to the quantity of the data, this increase is only on a small scale. As a result, the technique that has been presented is suitable for enormous volumes of big data. The amount of big data is substantial, and as a result, memory consumption is an important factor to consider when assessing the effectiveness of the suggested technique. As can be seen from the comparison findings presented in Figure 2, the work that is being suggested uses less RAM for the purpose of encrypting and storing data.

## VI DISCUSSION

A large number of people are able to view the public data since it has been put to the public cloud. Simply encrypting the information about the storage path index is all that is required to safeguard this public data. As a result of the large number of authorized users who have access to public data, the process of information sharing for encrypted storage indexes is straightforward. In contrast to the public data, which is not encrypted, the complete sensitive data as well as a portion of the insensitive data is encrypted. As a result of the fact that just the information on the storage index of public data is encrypted and shared among authorized users, the complexity of computation is also decreased. The results of the experiments demonstrate that the suggested approach is capable of providing enhanced throughput while simultaneously reducing memory use. To summarise, the work that has been suggested offers enhanced safety while also reducing the amount of required calculation.

## VII CONCLUSION

The most important addition is that this phase offers a technique that makes it easier to use a hybrid cloud platform for the purpose of maintaining and processing large datasets that contain sensitive, insensitive, and public data. The manner of dividing is determined by the significance of the data collected. When it comes to cloud storage, the PRE idea is utilized to safeguard the sensitive data of users. Re-encryption and the production of re-encryption keys are processes that are handled by the proxy server when PRE is applied to cloud storage. When it comes to sensitive data, this offers considerable benefits in terms of both security and privacy. Although it may appear that the implementation of PRE is a difficult task, the complexity of the process is insignificant when compared to the benefits that may be derived from securing sensitive data of cloud users. Encrypting certain random blocks and also encrypting the storage path index and sharing it with authorized users is the method that this study intends to utilize in order to safeguard data that is not very sensitive. It is not feasible to extract actual data while using random encryption of blocks since even if an intruder manages to access part of the blocks, they will not be able to access the contents. It is quite simple to encrypt and share the storage path index since its size is relatively little in comparison to the real data. This makes it possible to safeguard the data in a very straightforward manner.

## REFERENCE

[1] Lavin A. & Ahmad, S. (2015). Evaluating real-time anomaly detection algorithms--the Numenta anomaly benchmark, in IEEE 14th international conference on machine learning and applications (ICMLA), IEEE, pp. 38–44.

[2] Alouffi, B. Hasnain, M. Alharbi, A. Alosaimi, W. Alyami, H. & Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies, IEEE Access, vol. 9, pp. 57792–57807.

[3] Chu C.-K. and Tzeng W.-G. (2007). Identity-based proxy re-encryption without random oracles. In International Conference on Information Security, 189–202. Springer.

[4] Moore, D. Shannon, C. & Claffy, K. (2002). Code-Red: a case study on the spread and victims of an Internet worm, in Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment, pp. 273–284.

[5] Geetha Rani E. & Chetana, D. T. (2023). A Survey of Recent Cloud Computing Data Security and Privacy Disputes and Defending Strategies, in Congress on Smart Computing Technologies, Springer, pp. 407–418.

[6] Fernández A., del Río S., López V., Bawakid A., del Jesus M. J., Benítez J. M., and Herrera F., (2014). Big Data with Cloud Computing: an insight on the computing environment, MapReduce, and programming frameworks, Wiley Interdisciplinary Reviews: Data Mining

and Knowledge Discovery, 4(5), 380–409.

[7] Sharafaldin, I., Lashkari, A. H. & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp, vol. 1, pp. 108–116.

[8] Cup, K. D. D. (2007). Available on: http://kdd. ics. uci. edu/databases/kddcup99/kddcup99. html.

[9] Erhan L., et al. (2021). Smart anomaly detection in sensor systems: A multi-perspective review, Information Fusion, vol. 67, pp. 64–79.

[10] Frederick, M. (2023). Risk of Cloud Breaches Rising, Teams Struggling to Address Them, Fugue and Sonatype Survey Finds, Fugue and Sonatype. Accessed: [Online]. Available: https://www.fugue.co/press/releases/risk-of-cloud-breaches-rising-teams-struggling-to address-them-fugue-and-sonatype-survey-finds

[11] Ring, M., Wunderlich, S., Grüdl, D. Landes, D., & Hotho, A. (2017). Flow-based benchmark data sets for intrusion detection," in Proceedings of the 16th European conference on cyber warfare and security. ACPI, pp. 361–369.

[12] Tavallaee, M., Bagheri, E., Lu, W. & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set," in 2009 IEEE symposium on computational intelligence for security and defense applications, Ieee, pp. 1–6.

[13] Moustafa, N., & Slay, J. (2015). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set), in military communications and information systems conference (MilCIS), IEEE, pp. 1–6.

[14] Mell, P. & Grance, T. (2011). The NIST definition of cloud computing.

[15] Sadkhan, S. B. (2022). Security of Cloud Networks–Status, Challenges and Future Trends," in 2022 8th International Engineering Conference on Sustainable Technology and Development (IEC), IEEE, 2022, pp. 247–252.

[16] Alturfi, S. M., Al-Musawi, B., & Marhoon, H. A. (2020). An advanced classification of cloud computing security techniques: A survey," in AIP Conference Proceedings, AIP Publishing, 2020

[17] Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing.