International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 15 August 2023 **Revised:** 06 October 2023 **Accepted:** 20 October 2023*

Comparative Analysis of Data Security and Cloud Storage Models Using NSL KDD Dataset

Dinesh Parkash [1], Dr. Sumit Mittal [2]
[1]Research Scholar, MMICT & BM, Maharishi Markandeshwar (Deemed to be University),
Mullana, Ambala, Haryana, India
e-mail: dineshgcccs@gmail.com
[2]Professor, MMICT & BM, Maharishi Markandeshwar (Deemed to be University),
Mullana, Ambala, Haryana, India
e-mail: sumit.mittal@mmumullana.org

Abstract—Cloud computing is becoming increasingly important in many enterprises, and researchers are focusing on safeguarding cloud computing. Due to the extensive variety of service options it offers, A significant amount of interest from the scientific community has been focused on cloud computing. The two biggest problems with cloud computing are security and privacy. The key challenge is maintaining privacy, which expands rapidly with the number of users. A perfect security system must efficiently ensure each security aspect. This study provides a literature review illustrating the security in the cloud with respect to privacy, integrity, confidentiality and availability, and it also provides a comparison table illustrating the differences between various security and storage models with respect to the approaches and components of the models offered. This study also compares Naïve Bayes and SVM on the accuracy, recall and precision metrics using the NSL KDD dataset.

Keywords-SVM (Support Vector Machine), NB (Naïve Bayes), DoS (Denial of Service), NSL KDD Dataset.

I. INTRODUCTION

Cloud computing is accomplished through the utilization of remote servers and the Internet, a variety of services can be provided, that technology is called cloud computing. As long as a device can connect to the internet, it has access to the information and software it needs to function properly. Using cloud storage, we don't need to keep our data on our own private server or on any kind of local device. An IoT gadget can access information and the necessary software to function. Computing in the cloud has been designed with the intention of speeding up the rate of innovation, the flexibility of resources, and the economies of scale by making them available over the Internet ("cloud"). Infrastructure management is enhanced, operational expenses are reduced, and scalability is made possible by only paying for the cloud services actually used.[21]

A. History

In 1996, Compaq document, the phrase "cloud computing" initially used. The term "cloud" was first associated with the idea of cloud computing, which had previously been discussed in scientific works and gained importance inside Apple-founded General Magic at the very start of the 1990s. J.C.R. Licklider, the initial head of the Information Technology Methodologies Unit inside the Pentagon's ARPA organization in the 1960s, is said to have initially proposed the notion, according to Computer world. In 1969, Bob Taylor and Larry Roberts founded ARPANET (Advanced Research Projects Agency Networks) on the back of a revolutionary notion by J.C.R. Licklider.

B. Types of Cloud

- Private
- Public
- Hybrid
- Community
- Multi

a) Private

Distributed systems based on private infrastructure that allow for on-demand allocation of computer resources to end users are known as private clouds. Pay-as-you-go models could potentially be replaced in private clouds by alternative approaches that better control cloud consumption and proportionately bill different divisions or segments of an organization.
e.g. Private CSP(Cloud Service Provider) are Microsoft, HP data center and Ubuntu etc.

b) Public

Third-party cloud providers provide public cloud services via the internet, typically on a pay-as-you-go basis. They offer strategies for cutting down on the price of IT systems and

***Article Received:** 15 August 2023 **Revised:** 06 October 2023 **Accepted:** 20 October 2023*

evolving into a practical option for handling high demands on the local network. Public clouds are the preferred option for startups because they allow businesses to get up and running with minimal up-front expenditure by using existing public networks to handle all of their information technology needs. It's meant for a wide audience, not just one customer. Each user requires their own private and maybe isolated virtual machine.

c) Hybrid

A hybrid cloud is a combined distributed system that brings together the top features of public clouds and private clouds.

d) Community

These are geographically dispersed systems that are formed by integrating the capabilities of multiple clouds customized to meet the one-of-a-kind requirements of a certain area of industry, community, or commercial enterprise. They are created by integrating the capabilities of many clouds. Nevertheless, it is difficult for the corporations to divide the obligations between themselves. In this cloud, businesses who work on similar problems or projects pool their resources for their own infrastructures. A company or an outside entity could be responsible for managing the cloud.

e) Multi

The usage of several cloud computing offerings from different providers, known as multi-cloud, enables enterprises to make use of the most appropriate services for their individual needs while avoiding vendor lock-in. This enables enterprises to take use of the many features and capabilities provided by various cloud providers. Figure 1 has shown Cloud Development Models.[22]

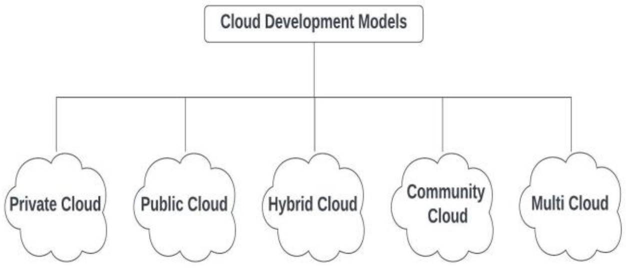

Figure 1: Cloud Deployment Models

C. Machine learning

The field of machine learning is the subfield of AI that enables computers to acquire new skills and knowledge from observation and experience rather than being given specific instructions. To put it another way, machine learning represents branch of AI that gives computers the ability to study and improve on their own. Through the technique of machine learning, a computer system acquires the ability to predict the future or perform certain decisions without being explicitly programmed to do so. To generate reliable findings or predictions from the data it is allowed access to, machine learning model needs an enormous quantity of data that is either completely or somewhat structured.

It has three distinct categories of learning:

- Supervised
- Unsupervised
- Reinforcement

a) SVM (Support Vector Machine)

We can perform tasks like Regression and Classification with the help of this approach for supervised machine learning. When analyzing data, SVM plots points in a two-dimensional (2D) space with as many dimensions as there are characteristics (n). Selecting a useful hyper-plane that partitions the classes cleanly is the next step in the classification process. SVM i.e. formally defined as a separation hyperplane, which makes it a discriminative classifier. As a result of labeled data used for training (supervised learning), the algorithm creates an optimal hyperplane for classifying new cases. The plane is divided in two by this hyperplane, a straight line in 2D space that represents the boundary between the two classes. Let's pretend, for the sake of argument, that we need to differentiate between the human and animal classes.

b) Naive Bayes

Classification algorithms belonging to the Naive Bayes family are grounded in Bayes' Theorem. This isn't a single algorithm; rather, there is a group of algorithms that share a common philosophy: that the independence of the pairs of characteristics being classified is a necessary condition for success. Naive Bayes relies on the assumptions that a) each feature is unrelated to the outcome and b) each feature contributes equally to the final result. The term "naive" (which means "innocent") refers to the fact that this is not true in the real world. Figure 2 has shown the types of Machine Learning.

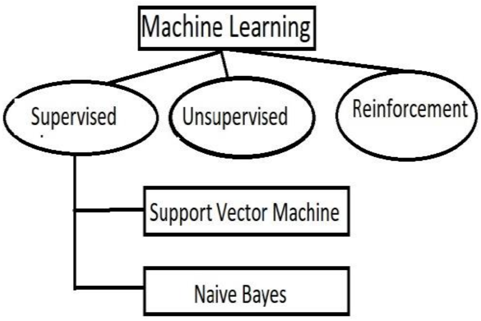

Figure 2 : Types of Machine Learning

D. Dataset

Datasets are collections of information that have been organized in some fashion. Anything from a sequence in an array to rows and columns in a database table might be part of a dataset. A tabular dataset can be visualized as a table or matrix where the columns represent variables and the rows represent fields. "Comma Separated File," or CSV, is the most widely accepted format for tabular datasets.

- *NSL KDD*

The initial data collection that was presented at KDD'99 has been revised and reintroduced as part of the NSL-KDD data set. Researchers have access to a trustworthy benchmark in the form of this data set, which they may use to evaluate the effectiveness of various intrusion detection technologies. There have been other datasets like NSL-KDD. Knowledge discovery and data mining tools competed for the KDD cup.
This contest was first run in 1999 to compile data on vehicle movements. The goal of the competition was to develop an intrusion detector for a network, a prediction model that could identify malicious connections (intrusions or attacks) from benign ones. Thousands upon thousands of internet traffic records were amassed for this competition and released as KDD'99 data set; from this came the NSL-KDD version of dataset, i.e. corrected and cleaned-up report of the file.

II. BACKGROUND STUDY

A lot of commendable research works have been carried out by the various researchers in the field of security issues, requirements needed for cloud computing environments. Sood, S. K. [1] proposed a framework to guarantee data protection in cloud computing environment. The framework involves classifying data based on three cryptographic parameters, using SSL encryption, MAC for integrity check, searchable encryption, along with dividing data into 3 sections for storage space. This paper also includes a summary of related work, a proposed model to solve the security issue, and a security analysis of the model Juels, A., & Kaliski, B. S. [2] Proofs of Retrievability (PORs) are a new type of cryptographic evidence that allow a file backup or archiving service to generate a short proof that a user may retrieve a specific file. The study looks at POR protocols where the storage needs of the user (verifier) and the prover are tiny and constant regardless of the file size. In addition to proposing novel, implementable POR designs and discussing technology concerns and optimizations based on formerly investigated, related schemes, this work also gives rise to a novel, unconventional notion of security. This eliminates the need for the user to obtain the material on one’s own. In addition to this, the study presents novel, implementable POR constructs and investigates practical considerations and optimizations based on comparable schemes that have been investigated earlier.

Chor, B. et al [3] methods were described that allow a user to privately retrieve data from k (k >=2) replicas of a database. The strategies rely on the replication to save a lot of money. In this paper, we describe a pair of servers approach due to the complexities of communication O(n(1/3)). Wang, C et al [4] a storage solution on the cloud was presented, it was suggested that a distributed memory integrity auditing technique be implemented. Users can do an audit of their cloud storage using the proposed method with low communication and computational overhead. In addition to reassuring consumers that the cloud securely stores their data, the audit's results can be used to quickly pinpoint the source of any data errors, such as a malfunctioning server. The suggested technique is both very effective and resistant to various types of assaults, including Byzantine a failure, malicious data change, and server collusion. This paper has practical implications for cloud storage service providers and users as it provides a secure and efficient mechanism for auditing cloud storage and ensuring availability and data integrity.

Wang, C et al [5] planned a distributed system using tokens of homomorphic and verification of erasure-coded data through distributed processes was provided as a technique for ensuring the precision of the information that is stored by users in environments that make use of cloud computing. The solution that has been provided is exceptionally effective and resistant to a wide variety of security risks. Additionally, dynamic operations such as and are supported by the techniques like updating, deleting, and appending data in a secure and fast manner. These operations can be performed on data blocks. The solution that has been provided is exceptionally effective and resistant to a wide variety of security risks. Prasad, P. et al [6] planned a framework designed for 3 Dimensional protections in Cloud Computing to address the crisis of data leakage. The framework works in 2 phases - data classification based on Integrity, Availability & Confidentiality and 3D technique for accessibility. In the first phase, the client categorizes the data based on its sensitivity and assigns a priority rating using a proposed formula. In the second phase, the 3D technique is used for accessing the data, which involves authentication and authorization of the user. Kamara, S. et al [7] proposed a number of different architectures, each of which combines new and non-standard cryptographic primitives, have been offered as potential solutions for building a secure cloud storage space service on top of an existing public cloud infrastructure. The paper describes designs for both consumer and enterprise scenarios. However, the paper does not provide any specific results or experimental data. Instead, it focuses on the profit such architecture would offer to mutually consumers and service providers. Singh, D., & Verma, H. K. [8] developed a novel approach for protecting data privacy within the cloud. Data kept in the cloud is saved private and unaltered by the proposed model's implementation of AES, SHA-1, and the Station-to-Station Key Agreement protocol. Each server in the cloud network serves as both a server for storing data and a server for authentication, and the servers are all interconnected in a ring. The following tasks are carried out by the servers: The station-to-station key agreement protocol begins with the server authenticating the user and the user authenticating the server. If the match is successful, the file is provided back to the user for verification, and if verification is successful, an error notice is sent to the user telling them that the data file has been edited or corrupted. The suggested system can serve both large businesses and individual consumers because to its reliability and low overhead. Bhandari, A. et al [9] an effective structure for the protection of data and the provision of storage space in cloud computing was proposed. The data that is being transferred, shared, and stored in data centers is protected from unauthorized access by the framework thanks to the classification of the data, the use of Hashing Communication Codes of authentication, as well as an indexing system. The information is presented in three distinct parts, namely public, private, and limited access, based on the cost of the function having C, I, and A represent Confidentiality, Integrity, and Availability, respectively. Protecting data when using cloud computing is possible with the help of the proposed framework, which is fetching gradually more popular due to its scalability and cost-effectiveness.

Zissis, D., & Lekkas, D. [10] proposed a security solution that leverages a reliable Outsider that can guarantee certain security characteristics within an environment that is hosted in the cloud. Protecting data when using cloud computing is possible with the help of the proposed framework, more especially Public Key Infrastructure working in conjunction with LDAP and SSO, in order to assurance the authentication, integrity, in addition to confidentiality of all data and communications that are relevant to the problem. This article conducts an analysis of cloud security by determining the specific security needs that must be met, and it offers a workable solution that gets rid of any potential dangers. The authors suggest the implementation of a Reliable Third Party, which would be assigned with the responsibility of ensuring certain security properties inside a cloud environment. The proposed approach makes use of cryptography, more particularly Infrastructure of public key working in combination among Single Sign On (SSO) along with lightweight directory access protocol (LDAP), in order to guarantee the authenticity, integrity, and secrecy of the data as well as communications that are at issue. The solution offers a horizontal level of service that is accessible by all entities that are involved. This level of service provides a security mesh within which critical trust can be preserved. Hussien, Z. A.et al [11] proposed an effective and reliable system for ensuring the safety of data within a third party auditor that is only partially trusted. The technique uses the curve of elliptic cryptography to provide confidentiality of data, correctness, and protection while transmitting data across unsafe channels, as well as an innovative encryption specification that preserves the privacy of data owner, an encryption hash function to preserve the integrity of data owner, and a cryptography hash function to preserve data owner integrity. Following the completion of the security analysis, it was determined that the suggested scheme is capable of withstanding a man-in-the-middle attack and produces proper data. However, the paper does not provide any specific results or experiments conducted to validate the proposed scheme. Wang, C.et al [12] planned a proposal that was made for a public auditing system that would protect users' privacy while ensuring the safety of cloud data storage. To achieve a secure public cloud data evaluating system, the system makes use of a public key-based homomorphic authenticator in conjunction among random masking. This satisfies all of the requirements for safely introducing a successful third party auditor (TPA) without requiring a local copy of the data and without introducing any new vulnerability to the user's data privacy. The suggested system expanded into multi-user surroundings utilizing the method of bilinear aggregate signature in order to facilitate efficient handling of many auditing activities. This was done to assist the system's overall purpose. The study presented a comprehensive analysis of both security and performance, demonstrating that the suggested strategies are both demonstrably safe and extremely effective. Caviglione, L.[13] studied the possible breach safety posed by covert routes in private cloud storage services, focusing primarily on Dropbox in this line of inquiry. The authors developed two distinct covert communication methods, which they referred to as REN (Renaming of File) and ALT (Alteration of File Method), and tested how well these approaches performed in terms of both bandwidth and robustness in various real-world settings. According to the findings, the proposed methods are capable of clandestinely transferring data over the web and can be utilized to construct a communication layer that enables malicious software to conceal its presence for extended periods of time. This paper highlights the need for improved security measures to prevent covert communication.

Li, J. et al [14] planned a scheme in favor of implementing attribute-based encryption (ABE), also called for scalable and fine-grained right to use control systems, in rank to ensure safe contact control in cloud computing environments. The suggested system enables user responsibility by means of traitor tracing and enforcing access policies that are determined by the characteristics of the data. By utilizing the broadcast encryption method, it is possible to provide effective support for together the consumer contribution and the user removal. Kumar, N. S. et al [15] discussed a method that is safe access control in cloud computing, scalable and fine-grained access control systems can be constructed using attribute-based encryption (ABE). The suggested system will enable user accountability by employing traitor tracking in order to enforce access controls that are based on data properties. Utilizing the broadcast encryption method provides support for both the user grant and the user revocation in an effective manner. G. Ateniese et al [16] suggested PDP model minimizes I/O costs and network connection overhead, making it suitable for big data sets in globally system of scattered storage. The server's overhead is relatively minor or perhaps constant, in contrast to being directly proportional to the amount of data. The conducted experiments involving the installation of E-PDP in the Linux operating system validate the viability of PDP and demonstrate that its operational efficiency is primarily constrained by disk input/output operations rather than cryptographic processing. Zhu, Y., and colleagues [17] established a cooperative provable data possession (CPDP) technique for the purpose of ensuring the data integrity of distributed cloud storage systems. The wholeness, knowledge reliability, and no-knowledge properties of the scheme are validated by the research utilizing a multiprover proof with no knowledge system. This demonstrates that the scheme is secure. The study also discusses the scheme's performance optimization mechanisms, namely an efficient approach for determining ideal parameter values for reducing the computing expenses for consumers and storage suppliers.

Lin, C. et al [18] suggested PDP, is a crucial part of the safety framework for cloud computing on mobile devices that deals with data. This paper presents two mobile provable data possession (MPDP) strategies with the goal of bolstering data integrity and efficiency in mobile cloud computing. The Boneh-Lynn-Shacham brief signature process is implemented in the hashed tree data arrangement used by these systems. Some of the methods in which the systems enable data dynamics include by outsourcing verification, block less verification, stateless verification, and dynamic data operations. The results of experiments demonstrate that these methods achieve a high level of accuracy within the data verification procedure while still maintaining a cheap cost for data transmission. Akhil, K. M. et al [19] discussed a method implementing the algorithm known as AES for data transit was proposed as a means of improving the data security provided by cloud storage. Because the suggested method prevents third-party auditors from gaining access to user data, it will be difficult for adversaries to decipher the information that is being conveyed. Cong Wang et al [20] discussed a decentralized protocol with homomorphic tokens with erasure-coded data verification was developed for use in cloud data storage with the intention of providing storage error localization and correctness insurance. In addition to that, the study delves into the requirement of employing blinded parities including the utilization of erasure-correcting code in order for distributed storage systems to be able to endure many failures. Parkash, D. & Mittal, S. [21] utilizing Cuckoo Search Algorithms, a novel strategy for Intrusion Detection Systems (IDS) was proposed, along with the development of a fresh fitness function. The aforementioned representation has been developed among regard to the KDD Cup 99 dataset in order to choose the features of the highest quality that best reflect qualitative data and to exclude redundancy from the dataset. The findings of this study indicate that a proposed secured framework to secure a Cloud computing environment that makes use of the Cuckoo Search Algorithm is successful in identifying intrusions and in elevating the level of security. Parkash, D. & Mittal, S. [22] proposed an efficient security structure via ABC in cloud computing. The planned approach has been taught with KDD99 dataset. The authors have utilized Artificial Bee Colony Algorithm for efficient security in cloud computing. We have randomly chosen features, and then we have utilized advancement procedure with ABC Algorithm. The proposed IDS performed better than Naïve Bayes and SVM IDS concerning Precision, Accuracy and Recall limits. We have prepared 36 preliminaries in their proposed IDS.

Zaman, S. & Karray, F.[23] suggested lightweight IDS is able to provide adequate system performance thanks to careful consideration of the features to be used and the IDS classification scheme. Training as well as testing times can be drastically cut with the features selection strategy thanks to the Fuzzy ESVDF algorithm. The IDS classification method improves the accuracy and generalizability of the system, making it easier for organizations to identify most forms of attack. The proposed system has been tested through several experiments, and it has been found to be effective. Haq, I. U. et al [24] proposed a hybrid distributed faith model that uses public key infrastructure (PKI) in addition to reputation-based faith structures for the purpose of validating hierarchical Service Level Agreement (SLA) aggregations across a performance-enriched environment that includes a network or a cloud environment. This model was developed in order to validate hierarchical SLAs. The methodology that is being presented helps to prevent SLA violations by identifying services that are more likely to be violated during the service selection process and by actively participating in violation management during the time when penalties are being enforced. In addition to that, this work presented the use of real-time validation of SLAs as a method for ensuring that the service assurances are fully compliant with the levels that were predicted. Habib, S. M. et al [25] suggested design for a Trust Management (TM) system that incorporates multiple facets, designed for use in a cloud computing market. The suggested approach makes it possible to determine which cloud service providers may be trusted in terms of a variety of characteristics, such as security, performance, and compliance, by evaluating data from a number of different sources and tracing its origins back to several trusted organizations. Additionally, the authors give the required tools for evaluating, expressing, and computing trust. They provide a concise overview of the internal components of the system and propose an innovative architecture for a TM system that is designed for use in cloud computing marketplaces. Pawar, P. S. et al [26] planned a trust model for cloud service providers based on reputation and uncertainty. The model uses subjective logic operators to calculate the reputation of cloud service suppliers based on existing facts. The planned model is evaluated as well as compared with existing reputation models. Habib, S. M. et al [27] planned architecture for a dependence managing system that takes into account multiple criteria, which include compliance, data governance, as well as data security that customers may use to determine whether cloud providers can be trusted. The suggested approach relies on data from the Consensus Assessment Initiative Questionnaire (CAIQ). Details on the application manager, faith computation engine, along with trust expression and visualization module are also included in the article. At the end of the paper, real-world datasets are used to conduct experimental evaluations of the suggested system. The investigational findings reveal the usefulness of the planned system in identifying trustworthy cloud suppliers based on several parameters while offering insights into the boundaries of the system in real-world use. Chong, S.-K. et al [28] proposed a multilevel faith management frame to progress the accuracy of faith evaluation between consumers and providers in service-oriented computing applications. The framework addresses the vulnerabilities of the current trust management system and introduced a novel interactive faith management approach to develop the accuracy in estimating faith information. The proposed framework uses a combination of different types of information to compute trust. The paper also discusses the challenges in designing a trust management model and proposes a mathematical verification function to determine the weight of the rating. However, this approach does not provide any specific outcome of the planned framework. Chong, S.-K. et al [29] suggested a multi-tiered architecture for managing trust in cloud computing marketplaces, including a filtering mechanism to assess the veracity of user reviews and a trust measure to rank the reliability of individual service providers. The planned technology is proficient to accurately identify potentially dangerous trades on the web. In addition to outlining what should be included in a trust management system, this article discusses the best practice of identifying and assessing the nature of security risks to the trust information at the outset of the project. However, the paper does not provide a detailed explanation of the methods used to develop the proposed trust management system. Noor, T. H. et al [30] cloud computing's trust management difficulties by proposing a framework based on reputation dubbed CloudArmor. An adaptive credibility model safeguards cloud services from malevolent users, while an availability model orchestrates the decentralized deployment of a faith management service, all inside a framework that ensures users' privacy. Prototype and experimental research employing real-world trust suggestions on cloud services verify the feasibility as well as advantages of the technique.

Table 1 : Comparison of Cloud Security and Storage Models

Sr. No.	Author	Techniques	Year	Privacy	Integrity	Confidentiality	Availability
1.	Chor, B. et al [3]	Replication and two server scheme	1998	✓	×	×	×
2.	Juels A. et al.[2]	cryptographic proof of knowledge (POK)	2007	✓	✓	×	✓
3.	G. Ateniese et al [16]	Provable facts Possession order	2007	×	✓	×	×
4.	Wang, C.et al [5]	Distributed scheme	2009	✓	✓	✓	✓
5.	Kamara S. et al [7]	Cryptographic Cloud Storage using symmetric encryption scheme	2010	✓	✓	✓	×
6.	Wang, C. et al [12]	Homomorphic authenticator and random masking	2010	✓	✓	✓	×
7.	Li, J. et al [14]	ABE	2010	×	×	✓	×
8.	Prasad, P. et al [6]	3 D technique	2011	✓	✓	✓	✓

Article Received: *15 August 2023* ***Revised:*** *06 October 2023* ***Accepted:*** *20 October 2023*

9.	Sood S.K. [1]	SSL (Secure Socket Layer), MAC (Message Authentication Code)	2012	✓	✓	✓	✓
10.	Wang, C.et al [4]	distributed scheme & integrity auditing	2012	✓	✓	✓	✓
11.	Zissis, D. et al [10]	Single Sign on, lightweight directory access protocol & predominant protocol	2012	✓	✓	✓	✓
12.	Zhu, Y., et al [17]	Supportive PDP Scheme	2012	✗	✓	✗	✗
13.	Hussien, Z. A.et al [11]	AES (advanced encryption standard), ECC (elliptic curve cryptography)	2015	✓	✓	✓	✗
14.	Kumar, N. S. et al [15]	ABE with hashfunctions, digital signature	2015	✓	✗	✗	✗
15.	Singh, D.et al [8]	AES, SHA-1	2016	✗	✓	✓	✗
16.	Bhandari, A. et al [9]	Hashed Message Authentication codes	2016	✓	✓	✓	✓
17.	Caviglione, L. et al [13]	Covert Communication	2016	✓	✗	✗	✗
18.	Lin, C. et al [18]	Mobile PDP Scheme	2017	✗	✓	✗	✗

Table 2 : Comparison of Trust Models based on Cloud Security

Sr. No.	Author	Year	Technique used	Model	Components	Type of Simulation
1.	Juels A.et al [2]	2007	symmetric-key cryptography and efficient error-coding	Sentinel-based POR Model	spot-checking and error-correcting code	Experimental values
2.	Cong Wang et al [20]	2009	flexible distributed scheme	Storage Correctness Model	Token Pre-computation, Correctness Verification & Error Localization Algorithm	Performance Evolution by Experimental values
3.	Zaman S. et al [23]	2009	Fuzzy Enhanced Support Vector Decision Function (ESVDF) algorithm & classification	lightweight IDS	features selection, Classification & Darpa KDD 99	Experimental Values
4.	Haq, I. U. et al [24]	2010	Policy & reputation based	Hybrid Distributed Trust Model	SLA, reputation and PKI	Case Study
5.	Habib, S. M. et al [25]	2011	Information filtering	Multifaceted Trust Model	CAIQ Engine, Trust manager, TSE,TCE and TUE	Questionnaire
6.	Pawar, P. S. et al [26]	2012	Reputation based	Uncertainty Model	SLA Monitoring, SP Rating, SP Behavior	3 Different Experiments
7.	Habib, S. M. [27]	2013	Consensus Assessment Initiative Questionnaire (CAIQ)	multi-faceted trust management system architecture	Registration Manager, Trust Computation engine & Trust	experimental validation

					Representation and Visualization Module	
8.	Chong, S. K. et al [28]	2013	Feedback related & filtering	Multilevel Trust Model	Verification & evaluation	Questionnaire
9.	Chong, S. K. et al [29]	2014	Feedback & filtering	Multi-attribute Trust Model	Access Control & Trust evaluation	Graphs by Simulation
10.	Noor, T.H. et al [30]	2014	Credibility trust feedbacks	Reputation-based Trust Management framework	CSP, Trust management Facility & Cloud Facility customer sheet	Experiment based evaluation
11.	Akhil, K. M. et al [19]	2017	(Advance Encryption Standard) AES Algorithm	AES based Secured Model implemented in Java platform	Encryption Algorithm and Cloud Authentication Server	Experimental Results
12.	Parkash D. et al [21]	2022	CSA algorithm	IDS Model	SVM, Naïve Bayes, KDD Cup 99	Using Python
13.	Parkash D. et al [22]	2023	ABC algorithm	IDS Model	SVM , Naïve Bayes, KDD Cup 99	Using Python

III. METHODOLOGY

In this section, we begin by processing the NSL KDD dataset. We have used the NSL KDD dataset to test the SVM and Naive Bayes classification algorithms and measured their accuracy, precision, and recall. Figure 3 has shown methodology used for both the models.

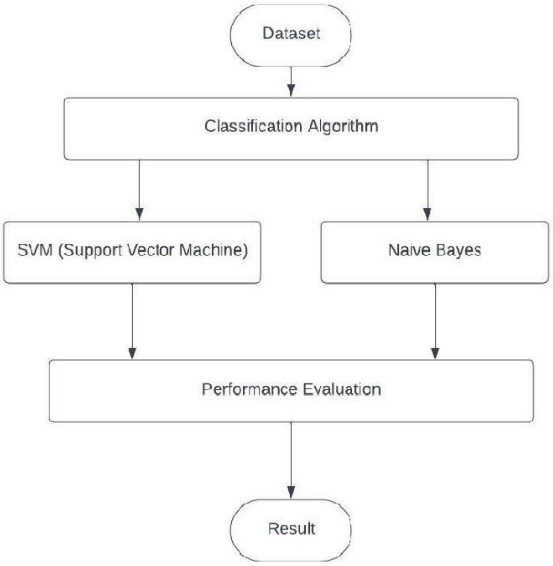

Figure 3 : Flow Chart of Methodology

IV. DATA ANALYSIS AND FINDINGS

The above experiment is performed on python using Intel(R) Core(TM) i5 -7300U CPU @ 2.60 GHz processor among 8GB RAM. In this experiment, we have taken (500-3000) test samples for the measuring the accuracy of the SVM along with Naïve Bayes. Table 1 and Table 2 have shown the comparison of cloud security and storage models. Also, a comparison of trust models based on cloud security has been carried out. Table 3 has shown the accuracy of SVM as well as Naïve Bayes in percentage. In the same way, we have also measured the precision and recall parameters in order to evaluate the performance of (500-3000) test samples. Tables 4 and 5 have shown the precision and recall in terms of percentage respectively. Figures 4, Figure 5 and Figure 6 have shown the percentage of accuracy, precision and recall parameter observations.

Table 3 : Accuracy (in percentage) of SVM Vs Naive Bayes

No. of Test Samples	**SVM Accuracy(%age)**	**Naïve Bayes Accuracy(%age)**
500	91	84
1000	87	85

***Article Received:** 15 August 2023 **Revised:** 06 October 2023 **Accepted:** 20 October 2023*

1500	88	80
2000	90	82
2500	89	78
3000	90	77

Table 4 : Precision (in percentage) of SVM Vs Naive Bayes

No. of Test Samples	SVM Precision	Naïve Bayes Precision
500	0.94	0.92
1000	0.89	0.88
1500	0.96	0.99
2000	0.90	0.92
2500	0.89	0.90
3000	0.91	0.89

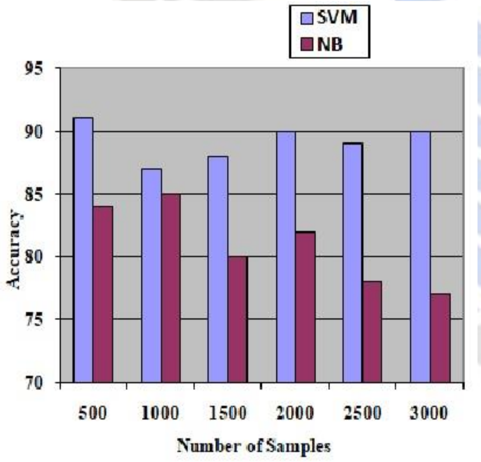

Figure 4 : Number of Test Samples versus Classification Accuracy for SVM Vs Naïve Bayes

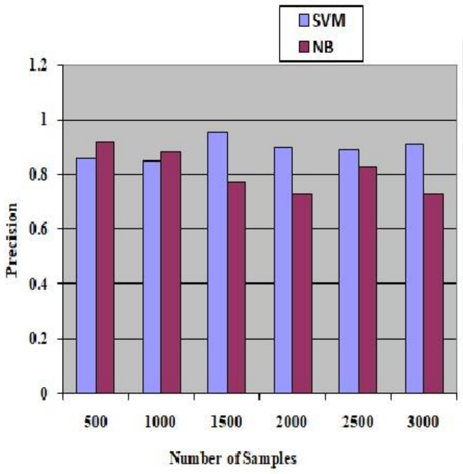

Figure 5 : Number of Test Samples versus Classification Precision for SVM Vs Naïve Bayes.

1500	0.88	0.77
2000	0.90	0.73
2500	0.94	0.83
3000	0.90	0.73

Table 5 : Recall of SVM along Vs Naïve Bayes.

No. of Test Samples	SVM Recall	Naïve Bayes Recall
500	0.86	0.73
1000	0.85	0.79

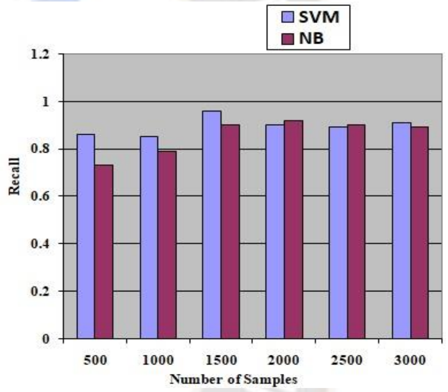

Figure 6 : Number of Test Samples versus Classification Recall for SVM along with Naïve Bayes

V. CONCLUSION AND DISCUSSION

The cloud computing infrastructure is already in place, and SDN is gaining popularity. Given their inevitable convergence as future enterprise IT solutions, it's important to examine how they might interact with one another, particularly in terms of network security. Using the NSL KDD dataset, we have analyzed the effects of cloud computing and SDN on distributed denial of service attacks. The trial helped us understand the potential of these edge-cutting tools. SVM and Naive Bayes have been used independently to evaluate the created system's accuracy. We have repeated the test Six times with the sample sizes (500-3000) to get a good sense of the system's reliability. SVM method has 90 percent of accuracy using 3000 test sample values. In the same way, value of precision and recall 0.9 and 0.9 have shown that SVM has performed better as compare to Naïve Bayes using NSL KDD dataset. The next step of our investigation will be to provide a more advanced data-secure framework in favor of the cloud computing.

REFERENCES

[1] Sood, S. K. (2012). A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35(6), 1831–1838. doi:10.1016/j.jnca.2012.07.007.

[2] Juels, A., & Kaliski, B. S. (2007). Pors. Proceedings of the 14th ACM Conference on Computer and Communications Security - CCS '07. doi:10.1145/1315245.1315317.

[3] Chor, B., Kushilevitz, E., Goldreich, O., & Sudan, M. (1998). Private information retrieval. Journal of the ACM, 45(6), 965–981. doi:10.1145/293347.293350.

[4] Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2012). Toward Secure and Dependable Storage Services in Cloud Computing. IEEE Transactions on Services Computing, 5(2), 220–232. doi:10.1109/tsc.2011.24.

[5] Wang, C, Wang Q, Ren K, Lou W. Ensuring data storage security in cloud computing, quality of service, 2009, IWQoS IEEE 17th international workshop, p. 1–9, 2009.

[6] Prasad, P., Ojha, B., Shahi, R. R., Lal, R., Vaish, A., & Goel, U. (2011). 3 dimensional security in cloud computing. 2011 3rd International Conference on Computer Research and Development. doi:10.1109/iccrd.2011.5764279.

[7] Kamara, S., & Lauter, K. (2010). Cryptographic Cloud Storage. Lecture Notes in Computer Science, 136–149. doi:10.1007/978-3-642-14992-4_13.

[8] Singh, D., & Verma, H. K. (2016). A new framework for cloud storage confidentiality to ensure information security. 2016 Symposium on Colossal Data Analysis and Networking (CDAN). doi:10.1109/cdan.2016.7570933.

[9] Bhandari, A., Gupta, A., & Das, D. (2016). A framework for data security and storage in Cloud Computing. 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT). doi:10.1109/icctict.2016.7514542.

[10] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583–592. doi:10.1016/j.future.2010.12.006.

[11] Hussien, Z. A., Jin, H., Abduljabbar, Z. A., Hussain, M. A., Abbdal, S. H., & Zou, D. (2015). Scheme for ensuring data security on cloud data storage in a semi-trusted third party auditor. 2015 4th International Conference on Computer Science and Network Technology (ICCSNT). doi:10.1109/iccsnt.2015.7490948

[12] Wang, C., Wang, Q., Ren, K., & Lou, W. (2010). Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. 2010 Proceedings IEEE INFOCOM. doi:10.1109/infcom.2010.5462173.

[13] Caviglione, L., Podolski, M., Mazurczyk, W., & Ianigro, M. (2017). Covert Channels in Personal Cloud Storage Services: The Case of Dropbox. IEEE Transactions on Industrial Informatics, 13(4), 1921–1931. doi:10.1109/tii.2016.2627503.

[14] Li, J., Zhao, G., Chen, X., Xie, D., Rong, C., Li, W.,Tang, Y. (2010). Fine-Grained Data Access Control Systems with User Accountability in Cloud Computing. 2010 IEEE Second International Conference on Cloud Computing Technology and Science. doi:10.1109/cloudcom.2010.44.

[15] Kumar, N. S., Lakshmi, G. V. R., & Balamurugan, B. (2015). Enhanced Attribute Based Encryption for Cloud Computing. Procedia Computer Science, 46, 689–696. doi:10.1016/j.procs.2015.02.127.

[16] G. Ateniese, R.C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J. Peterson, and D.X. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.

[17] Zhu, Y., Hu, H., Ahn, G.-J., & Yu, M. (2012). Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage. IEEE Transactions on Parallel and Distributed Systems, 23(12), 2231–2244. doi:10.1109/tpds.2012.66.

[18] Lin, C., Shen, Z., Chen, Q., & Sheldon, F. T. (2017). A data integrity verification scheme in mobile cloud computing. Journal of Network and Computer Applications, 77, 146–151. doi:10.1016/j.jnca.2016.08.017

[19] Akhil, K. M., Kumar, M. P., & Pushpa, B. R. (2017). Enhanced cloud data security using AES algorithm. 2017 International Conference on Intelligent Computing and Control (I2C2). doi:10.1109/i2c2.2017.8321820.

[20] Cong Wang, Qian Wang, Kui Ren, & Wenjing Lou. (2009). Ensuring data storage security in Cloud Computing. 2009 17th International Workshop on Quality of Service. doi:10.1109/iwqos.2009.5201385.

[21] Parkash, D., Mittal, S. (2023). An Enhanced Secure Framework Using CSA for Cloud Computing Environments. In: Gupta, D., Khanna, A., Bhattacharyya, S., Hassanien, A.E., Anand, S., Jaiswal, A. (eds) International Conference on Innovative Computing and Communications. Lecture Notes in Networks and Systems, vol 471. Springer, Singapore. https://doi.org/10.1007/978-981-19-2535-1_27.

[22] Parkash D.,Mittal S.(2022), "An Efficient Security Framework Using ABC in Cloud Computing." 2nd International Conference on Research Trends in Engineering and Management, Proceedings of ICRTEM-2022,(60-64).

[23] Zaman, S., & Karray, F. (2009). Lightweight IDS Based on Features Selection and IDS Classification Scheme. 2009 International Conference on Computational Science and Engineering. doi:10.1109/cse.2009.180.

[24] Haq, I. U., Alnemr, R., Paschke, A., Schikuta, E., Boley, H., & Meinel, C. (2010), "Distributed Trust Management for Validating SLA Choreographies", Grids and Service-Oriented Architectures for Service Level Agreements, Springer Science and Business Media, LLC 2010, 45–55.

[25] Habib, S. M., Ries, S., & Muhlhauser, M. (2011), "Towards a Trust Management System for Cloud Computing.", 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications.

[26] Pawar, P. S., Rajarajan, M., Nair, S. K., & Zisman, A. (2012). Trust model for optimized cloud services. In Trust Management VI: 6th IFIP WG 11.11 International

Conference, IFIPTM 2012, Surat, India, May 21-25, 2012. Proceedings 6 (pp. 97-112). Springer Berlin Heidelberg.

[27] Habib, S. M., Ries, S., Mühlhäuser, M., & Varikkattu, P. (2013). Towards a trust management system for cloud computing marketplaces: using CAIQ as a trust information source. Security and Communication Networks, 7(11), 2185–2200. doi:10.1002/sec.748

[28] Chong, S. K., Abawajy, J., Hamid, I. R. A., & Ahmad, M. (2014). A multilevel trust management framework for service oriented environment. Procedia-Social and Behavioral Sciences, 129, 396-405.

[29] Chong, S. K., Abawajy, J., Ahmad, M., & Hamid, I. R. A. (2014). Enhancing trust management in cloud environment. Procedia-Social and Behavioral Sciences, 129, 314-321.

[30] Noor, T. H., Sheng, Q. Z., Yao, L., Dustdar, S., & Ngu, A. H. (2015). CloudArmor: Supporting reputation-based trust management for cloud services. IEEE transactions on parallel and distributed systems, 27(2), 367-380.