International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

Optimizing Healthcare Data Management in the Cloud: Leveraging Intelligent Schemas and Soft Computing Models for Security and Efficiency

Krishna Chaitanya Rao Kathala, Ranadeep Reddy Palle

Abstract: ***Cloud computing plays a pivotal role in advancing the revolution of sensitive information management within the healthcare sector, facilitating the global exchange of health records through electronic means. Managing vast volumes of healthcare data is a monumental task, considering the multitude of patients whose information must be securely stored for future use. To address these challenges, the healthcare industry is increasingly integrating cloud computing into its systems for enhanced efficiency. This study focuses on evaluating the implementation of cloud computing for the management of extensive data in the healthcare sector. To tackle this objective, we propose an intelligent optimal schema that leverages soft computing models for the classification and management of vast sensitive data in the cloud. The approach begins with the introduction of the smart flower optimization (SFO) algorithm, specifically designed to optimize the cloud central server. This optimization ensures system scalability while concurrently reducing user access time and communication delays. Additionally, a time - limited optimal access control mechanism is employed to safeguard data privacy. The snow leopard optimization (SLO) algorithm is applied to data access, mitigating security flaws and enhancing privacy. Intensive execution appraisals approve the adequacy of the proposed structure, uncovering exceptional exactness, accuracy, review, and F1 - score upsides of 96.16%, 96.44%, 95.83%, and 96.14%, individually. These results emphasize the framework's exceptional capabilities in safeguarding sensitive healthcare data within the cloud computing platform from unauthorized access and maintaining its confidentiality.***

Keywords: vast sensitive, data management, data security, cloud computing, soft computing

1. Introduction

Organizations handle a vast array of data encompassing personal, professional, medical, and other sensitive information about their customers and users [1]. Entrusting the responsibility of managing such confidential data to organizations, customers rely on secure storage and maintenance. In the past, customer data was stored in dedicated centralized servers, presenting a vulnerability to single - point failures [2]. To address this, distributed environments emerged, distributing data across geographically dispersed servers. However, as data volumes increased, both centralized and distributed systems faced challenges related to space complexity. The advent of cloud environments offered a solution, enabling organizations to store their data in the cloud and allowing users to access it through various services [3]. Despite its advantages, the cloud environment is not immune to security threats, arising from both malicious and genuine registered users. Threats to data and services often result from rigid access restriction schemes, which can be enforced through various approaches such as feature - based, role - based, and profile - based methods [4]. Feature - based approaches validate user access before granting it, while role - based approaches consider the user's role in determining access. Profile - based approaches scrutinize user profiles to restrict access [5]. However, these methods struggle to achieve robust resistance against tampering and attacks by adversaries.

Ensuring data accessibility is paramount in cloud computing [6]. To provide continuous access, cloud providers often implement redundancy and failover measures, even in the face of hardware problems or outages. Striking a delicate balance between guaranteeing availability and maintaining security is crucial, as heightened security measures could potentially hinder data accessibility or render it unavailable [7]. The test is intensified by different information assurance regulations, adding intricacy to get information capacity in the cloud close by specialized obstacles. Notwithstanding specialized difficulties, the shift to distributed storage presents security concerns, particularly in shielding the privacy and trustworthiness of delicate information put away on remote cloud servers. To effectively combat the ever - changing landscape of online threats, robust encryption and access control systems are required [8].

In the contemporary business landscape, effective data management is a primary focus for industries seeking to enhance performance and meet consumer demands. Many industries and large organizations are actively exploring the implementation of diverse data management platforms to uphold their reputation among stakeholders and positive business environment [9]. Among these sectors, the healthcare industry stands out, dealing with various data sets that require meticulous maintenance to enhance service delivery. Efficient data management coupled with cloud computing proves to be advantageous for multiple facets of the healthcare industry, aiding in the effective handling of vast amounts of data and facilitating improved analytics. In recent times, various units within the healthcare sector have embraced cloud computing technology to elevate work culture and address systemic challenges [10]. The adoption of cloud computing not only provides seamless access to information but also offers a cost - effective solution, making it preferred choice for organizations navigating the current economic landscape. This study aims to explore and elucidate the utility of cloud computing in the healthcare sector.

Our contributions

We introduce an intelligent optimal schema that utilizes soft computing models for the efficient classification and management of extensive sensitive data within the cloud.

The primary contributions of the proposed schema can be outlined as follows:

1) Specifically crafted for optimizing the cloud central server, the smart flower optimization (SFO) algorithm ensures enhanced system scalability. Simultaneously, it reduces user access time and minimizes communication delays.
2) Implemented to safeguard data privacy, this mechanism incorporates the snow leopard optimization (SLO) algorithm for data access. The use of SLO helps mitigate security flaws, thereby fortifying privacy measures.

The subsequent sections of the paper follow this structure: Section 2 provides an overview of recently introduced schema for vast sensitive data management in cloud computing. Section 3 delves into the problem definition, framework model, and the upsides of the proposed system. Area 4 presents the outcomes and behaviors similar examination. At last, Area 5 finishes up this work.

2. Related works

2.1 State - of - art works for intrusion detection and diagnosis for cloud attacks

Xu et al. [11] have proposed a cloud environment based on semantics to make it easier to look through and analyze surveillance video data. A design coordinating cosmology building, semantic comment, and semantic hunt is utilized to use the semantic depiction of the video information to find them from idea based level. A semantic middle of the road layer which puts together the video information in light of their semantic relations is given. The essential central question and principal advancement of cloud is the combination of video understanding and semantic web innovations. The semantic web technologies are used for representing and organizing the huge number of video data.

Jiang et al. [12] have presented an information logical calculation which makes due, questions, and cycles unsure enormous information in cloud conditions. It processes the user - specified constraints to discover useful information and knowledge from the uncertain big data, allows users to query these big data by specifying constraints that express their interests, and manages transactions of uncertain big data. As everything in each exchange in these unsure huge information is related with an existential likelihood esteem communicating the probability of that thing to be utilized in a specific exchange, calculation could be serious. The MapReduce model on a cloud climate is utilized for viable information investigation on these unsure large information.

Noor et al. [13] have designed a standing based trust the executives (CloudArmor) structure that gives a bunch of functionalities to convey TaaS. The convention is utilized to demonstrate the believability of trust inputs and save clients' security. A versatile and powerful validity model is utilized for estimating the believability of trust inputs to shield cloud administrations from noxious clients and to think about the reliability of cloud administrations. The trust management service's decentralized implementation's availability is managed by means of an availability model.

Xia et al. [14] have presented a safe, ranked search scheme for multiple keywords over encrypted cloud data that simultaneously supports dynamic update operations like document deletion and insertion. In order to construct an index and generate queries, the widely used TF - IDF model and the vector space model are combined. They build a unique tree - based list construction and utilize an eager profundity first hunt calculation to give proficient multi - catchphrase positioned search. The solid kNN calculation is used to scramble the list and inquiry vectors, and in the interim guarantee exact significance score computation between encoded file and question vectors.

Meharwade et al. [15] proposed a framework that works with multi - proprietor watchword positioned search over scrambled cloud information, consolidating a vigorous key administration plot. To upgrade information recovery proficiency from an encoded information assortment, our methodology embraces the idea of a positioned accessible symmetric encryption model with a few enhancements. The framework is intended to effectively recover records containing data connected with a predetermined catchphrase in rank request from an encoded document assortment, focusing on records with more pertinent data about the word. The framework upholds various information proprietors for record transfers and executes a sound key administration conspire with further developed list building execution. Besides, it considers documents that contain more data connected with a word yet have less events of the word inside the record, doling out need to documents in light of their significance to the predefined catchphrase.

Malhotra et al. [16] have analyzed security concerns in various layers of cloud databases and examined proposed solutions for these issues. The external layer specifically deals with security matters related to authentication and access control. The researchers also evaluated solutions put forth by authors, including encryption techniques, querying encrypted data, Shamir's secret sharing algorithm, and a metadata approach. In this system, distinct data owners employ different secret keys to encrypt their documents and keywords. Authorized users can then perform queries without needing to know the keys of these various data owners.

Rajabzadeh et al. [17] have proposed to minimize energy consumption and reduce violations of service level agreements (SLA). The challenges related to the allocation and management of virtual machines are broken down into smaller components. The method carries out all the necessary steps in a distributed manner and only switches to a centralized mode when placing virtual machines that need a global perspective. The placement policy for virtual machines utilizes a population - based or parallel simulated annealing (SA) algorithm within the Markov chain model.

Arianyan et al. [18] have proposed proactive online resource management policies to improve energy efficiency, meet service level agreements (SLA), and minimize the number of migrations in cloud data centers. It uses a prediction algorithm to identify overloaded hosts and employs new decision - making techniques that consider multiple criteria to select virtual machines. The core concept of the EO

policy is to address the resource allocation issue for virtual machines (VMs) selected for migration from either overloaded or under - loaded physical machines (PMs) in a single step rather than handling each one separately. Simulation results using the CloudSimsimulator indicate a significant 98.11% reduction in the output metric, which represents energy consumption. .

Raza et al. [19] have investigated the security issues within a cloud environment and put forward a detailed security framework. It thoroughly examined all important aspects of security, assessing potential threats and suggesting defensive measures. The primary worry revolves around the fact that storing data in the cloud means clients may lose control over it. When an organization embraces cloud computing without proper security measures, it raises concerns. A private cloud, on the other hand, is considered more secure because everything—infrastructure, hardware, and applications—is kept separate from other organizations or users. The framework consists of guidelines designed to effectively protect the organization's data and applications. It uses a layered security structure to achieve the highest level of security, aiming to minimize the impact of potential threats.

Sighom et al. [20] have suggested a model that uses a mix of AES - 256, IDAs, and SHA - 512 for encoding and decoding data locally. The encoding process involves three main steps: first, applying AES - 256 encryption to secure the data; then, using IDA with Cauchy Reed–Solomon code to divide the encrypted data into multiple slices (n) that can be recovered from a subset (m); and finally, employing the SHA - 512 hashing algorithm for creating a signature. The decoding process involves several steps. First, there's a verification step to ensure the integrity of the data slices. Then, using IDAs (information dispersal algorithms), the encrypted data is reconstructed from multiple slices. Finally, the decryption process is applied to retrieve the original data.

2.2 Research gaps

The paramount concern is the safeguarding of privacy and security, requiring the development of robust encryption and sophisticated access control strategies to prevent unauthorized access and ensure the confidentiality of sensitive information. Scalability and performance issues must be addressed through the design of cloud infrastructures that can efficiently scale to accommodate the growing volume of sensitive data while maintaining optimal performance levels [21]. The development of optimization techniques is imperative to enhance the speed and efficiency of data retrieval processes, particularly for handling extensive datasets. Efficient data classification and indexing mechanisms are fundamental to support rapid and accurate data retrieval based on user queries. The challenge lies in creating effective indexing systems and automated techniques for classifying sensitive data, ensuring streamlined organization and management. Furthermore, the enhancement of keyword search algorithms is crucial, necessitating the development of advanced ranked search approaches that prioritize relevant results based on user queries. Investigating context - aware retrieval methods can further refine the accuracy and relevance of search results. The key management challenges arise, demanding innovative solutions for secure collaboration and conflict resolution. Addressing data ownership and governance concerns involves the establishment of reliable methods for verifying data ownership and the formulation of governance policies dictating how sensitive data is handled, shared, and retained within the cloud. Performance monitoring and optimization are critical aspects, requiring the development of tools for real - time monitoring and dynamic resource allocation to optimize cloud resource usage based on varying data processing demands. The user experience and interactivity aspects also demand attention, with a focus on designing user - friendly interfaces that provide an intuitive and seamless experience for interacting with sensitive data in the cloud. Additionally, the enhancement of query languages to support complex queries and foster improved user interaction with large datasets is vital. By addressing these multifaceted research problems, advancements can be made towards the creation of more efficient, secure, and user - friendly solutions for the effective management of vast sensitive data within cloud environments.

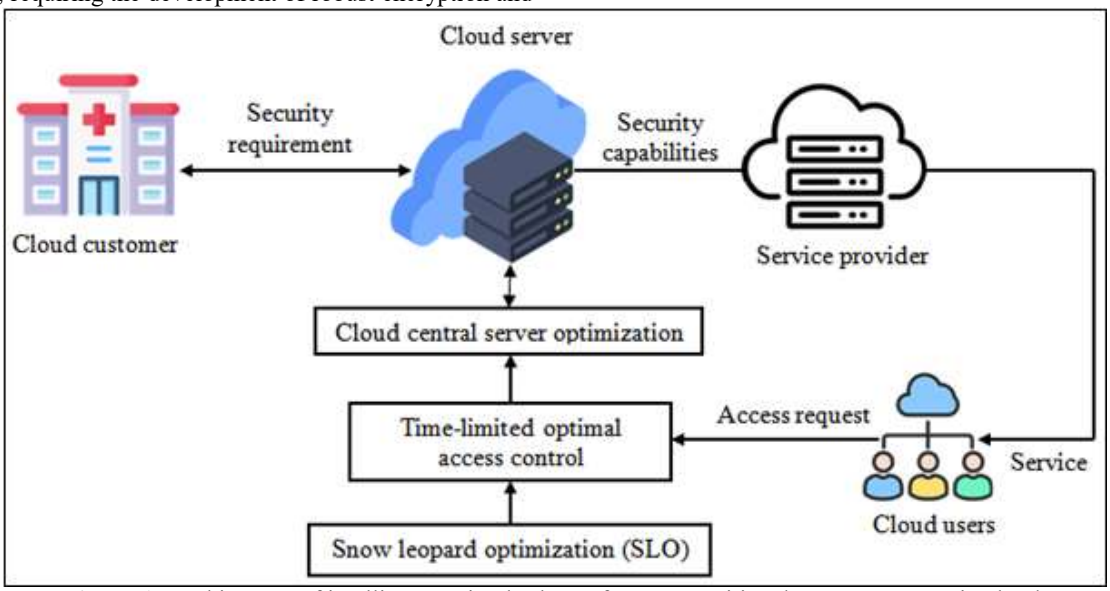

Figure 1: Architecture of intelligent optimal schema for vast sensitive data management in cloud

3. Proposed Methodology

3.1 Background study

At the beginning of our model, we start by offering a Security - as - a - Service framework for customers using the snow leopard optimization (SLO) algorithm. This helps create customized security setups or levels that match the specific requirements of the customers and take advantage of the capabilities provided by the cloud provider. During this phase, cloud customers have the autonomy to select desired security mechanisms, configure controls, and define policies based on the available services offered by the provider. The detailed process of establishing these security rings is illustrated in Fig.1. The smart flower optimization (SFO) algorithm undergoes updates in response to potential security policies, aligning with the service provider's capabilities, including the addition or removal of mechanisms. Usually, these updates happen at the most basic level of the service level objective (SLO). This involves either adding or removing new categories, which then has an impact on related categories at higher levels through the concept of inheritance. In the end, the main category of the best solution is updated, and it produces an efficient way to handle large amounts of sensitive data for cloud users with the most recent changes. This created system is then provided to the cloud user through an API, enabling them to choose the right security measures for each protocol according to their particular needs.

3.2 Optimize cloud central server

The optimization of the cloud central server is initiated with the introduction of the smart flower optimization (SFO) algorithm. This algorithm is meticulously crafted to enhance the efficiency and performance of the cloud central server. The primary objective is to achieve optimal scalability of the entire system, ensuring that it can seamlessly adapt and handle increased workloads or demands. Simultaneously, the SFO algorithm plays a crucial role in minimizing user access time, ensuring that users can retrieve or interact with data swiftly. Additionally, it addresses communication delays, streamlining the flow of information within the cloud environment. The SFO algorithm, through its intelligent optimization mechanisms, contributes to the overall effectiveness and responsiveness of the cloud central server. A population - based optimization algorithm is the smart flower optimization (SFO) algorithm. For the SFO, refreshing inquiry specialists should be possible in light of the development systems of the youthful sunflower. In this calculation, each juvenile sunflower is expected to have a stem length in a Faint layered search space. Since the SFO algorithm is a populace based calculation, the arrangement of the juvenile sunflowers can be addressed in a lattice as follows:

$$SF = \begin{bmatrix} sf_{1,1} & sf_{1,2} & \cdots & \cdots & sf_{1,Dim} \\ sf_{2,1} & sf_{2,2} & \cdots & \cdots & sf_{2,Dim} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ sf_{N,1} & sf_{N,2} & \cdots & \cdots & sf_{N,Dim} \end{bmatrix} \quad (1)$$

where Dim is the number of variables and N is the number of immature sunbirds. The stem length of each miniature sunflower in the proposed SFO algorithm is a solution to the optimization problem. The fitness value of each sunflower is proportional to the value of the optimization problem's objective function, which indicates the length of its stem. The primary method of the proposed Couch has been resubmitted.

$$K_{new,SF}^{Oye+1} = \begin{cases} K_{old,SF}^{Oye} + f \times \sin(\sigma) \times \left[Aux \times K_{best,SF}^{Oye} - K_{old,SF}^{Oye} \right], hours\,day \le 24 \\ K_{old,SF}^{Oye} + f \times \sin(\sigma) \times \left[K_{Best,SF}^{Oye} - K_{old,SF}^{Oye} \right], \quad otherwise \end{cases} \quad (2)$$

The following equation is used to adaptively decrease the parameter f during iterations:

$$f = damping_{\max} - Oye \times \frac{(damping_{\max} - damping_{\min})}{Oye_{\max}} \quad (3)$$

where $damping_{\max}$, $damping_{\min}$ are the greatest and small scale mum benefits of damping boundary, Oye signifies the dog lease cycle, and $Oye_{\max}$ implies the most extreme number of emphases.

$$K_{new}^{Oye} = K_{old,SF}^{Oye} + f \times \sin(\sigma) \times \left[K_{best,SF}^{Oye} - K_{old,SF}^{Oye} \right] at\ any\ hours\,day \quad (4)$$

In order to demonstrate that the hormone is not activated on a cloudy or rainy day, the effect of the "Aux" parameter has been eliminated from this equation.

4.2 Optimal access control mechanism

A time - limited optimal access control mechanism is a security feature designed to regulate and control access to sensitive data within a specified time frame. The mechanism ensures that users or entities can only access certain information or perform specific operations for a predetermined period. Once the allocated time expires, access privileges are revoked or restricted. This approach adds an extra layer of security by imposing time constraints on data access, mitigating the risk of unauthorized or prolonged access to sensitive information. The time limitation is a strategic measure to enhance security, especially in scenarios where temporary or restricted access is deemed necessary. This mechanism operates within a specified time frame, adding an extra layer of control and ensuring that access to sensitive data is regulated effectively. The snow leopard optimization (SLO) algorithm is

harnessed to orchestrate this access control mechanism. SLO, known for its efficiency in optimization tasks, is strategically employed to enhance the security posture of data access within the cloud environment. By leveraging the SLO algorithm, the access control mechanism addresses potential security flaws that may arise during data retrieval or utilization. The algorithm optimizes the access control process, making it more robust and resistant to vulnerabilities. Furthermore, the mechanism prioritizes and enhances privacy measures, ensuring that sensitive data is accessed and handled with the utmost confidentiality. In the SLO algorithm, each snow panther is an individual from the calculation populace. A specific number of snow panthers are individuals from SLO as search specialists. In populace improvement calculations, the individuals from the populace are distinguished by a lattice called the populace network.

$$Z=\begin{bmatrix} Z_1 \\ \vdots \\ Z_u \\ \vdots \\ Z_M \end{bmatrix}_{M\times n}=\begin{bmatrix} z_{1,1} & \cdots & z_{1,f} & \cdots & z_{1,n} \\ \vdots & \ddots & \vdots & & \vdots \\ z_{i,1} & \cdots & z_{u,f} & \cdots & z_{u,n} \\ \vdots & & \vdots & \ddots & \vdots \\ z_{M,1} & \cdots & z_{M,f} & \cdots & z_{M,n} \end{bmatrix}_{M\times n} \quad (1)$$

where Z is the number of inhabitants in the snow panther, Z_u is the I - th snow panther, Z_u d is the worth of the issue variable given by the f - th snow panther, M is the quantity of snow panthers snow panthers in the calculation populace, and m is the quantity of snow panthers issue factors.

$$D=\begin{bmatrix} d_1 \\ \vdots \\ d_u \\ \vdots \\ d_M \end{bmatrix}_{M\times 1}=\begin{bmatrix} d(Z_1) \\ \vdots \\ d(Z_u) \\ \vdots \\ d(Z_M) \end{bmatrix}_{M\times 1} \quad (2)$$

where D is the vector of the goal capability and d_u is the worth of the goal capability of the issue got from the u - th snow panther. This phase of the proposed SLO is demonstrated numerically as follows.

$$z_{u,f}^{O1}=z_{u,f}+t\times\left(z_{d,f}-U\times z_{uf}\right)\times sign\left(D_u-D_l\right),$$
$$l\in 1,2,3,....,M,\ f=1,2,3,...,n \quad (3)$$

$$Z_u=\begin{cases} Z_u^{o1}, D_u^{o1}\le D \\ Z_u, \quad else \end{cases} \quad (4)$$

$$U=round(1+t) \quad (5)$$

where Z_u^{o1} is the new worth of the f - th task variable got by the uth snow panther in view of stage 1, t is an irregular number in the span [0, 1], l is the column number of the chose snow panther. The u - th snow panther on the f - th hub, Z_u^{o1} is the refreshed area of the U - th snow panther in light of stage 1, and D_u^{o1} is the worth of its goal capability. For this, the proficient update is utilized, in which another position is satisfactory for an individual from the calculation in the event that the worth of the goal capability in the new position is more reasonable than in the past position.

$$o_{u,f}=z_{h,f}\ f=1,2,3,....,n \quad (6)$$

$$z_{u,f}^{o2}=z_{u,f}+t\times\left(\left(o_{u,f}-z_{u,f}\right)\times o+\left(o_{u,f}-2\times z_{u,f}\right)\times(1-f)\right)\times sign\left(D_u-D_o\right) \quad (7)$$

$$Z_u=\begin{cases} Z_u^{o1}, D_u^{o1}\le D_u \\ Z_u, \quad else \end{cases} \quad (8)$$

where pi, d is the dth aspect of the snow panther's prey area, Fp is the worth of the goal capability in light of the prey area, x P2 i, d is the new worth of issue variable d got with the ith snow panther. In stage 2, we compute the objective function which is worth of goal capability. The proliferation cycle of snow panthers is numerically displayed in view of the above ideas utilizing the condition.

$$v_k=\frac{z_k+z_{m-k+1}}{2},k=1,2,3,....,\frac{m}{2} \quad (9)$$

The time - limited optimal access control mechanism, empowered by the SLO algorithm, plays a pivotal role in fortifying data security and privacy within the cloud computing framework.

4. Results and Discussion

In this research, we discuss the results and comparative analysis of new and smart ways to handle large amounts of sensitive data in the cloud. We assess how well these approaches perform compared to the ones that are already in use. We carried out the tests on a computer running Windows 7. The computer had an 8 - core Intel Xeon E5 - 1620 processor, which runs at a speed of 3.50 GHz, and it had 32 GB of memory. Each server used in the experiment had a data transfer rate of 1 gigabit per second (1 Gbps). Half of this bandwidth was dedicated to moving data between servers, and the other half was used for virtual machine communication in the simulations. The simulation lasted for 86, 400 seconds. To better assess how well virtual machine consolidation performs, 600 servers had two processing cores, and the rest had only one. Each processing core in group G4 had a speed of 1, 860 million instructions per second (MIPS) and a memory capacity of 4096 megabytes (MB). In group G5, each core operated at 2660 MIPS with the same memory capacity of 4096 MB. We evaluated the outcomes of the SFO - SLO approach and compared them to several existing methods, such as simulated annealing (SA - SLA), multi - criteria TOPSIS with prediction VM selection (MTPVS - SLA), artificial neural network (ANN - SLA), dispersal algorithms and secure hash algorithm - 512 (DA - SHA - 512), and policy management engine (PME).

Table 1: Accuracy comparison

Schemas	Number of requests				
	500	1000	1500	2000	2500
SA - SLA	78.278	77.945	77.815	77.722	77.605
MTPVS - SLA	81.936	81.603	81.473	81.380	81.263
ANN - SLA	85.594	85.261	85.131	85.038	84.921
DA - SHA - 512	89.252	88.919	88.789	88.696	88.579
PME	92.910	92.577	92.447	92.354	92.237
SFO - SLO	96.568	96.235	96.105	96.012	95.895

Table 1 presents a comprehensive accuracy comparison among different schemas, each evaluated under varying numbers of requests. The results reveal notable variations in performance across the schemas. Starting with SA - SLA, the accuracy ranges from 78.278% to 77.605% as the number of requests increases. MTPVS - SLA demonstrates a slightly higher accuracy, with values ranging from 81.936% to 81.263%. Moving on to ANN - SLA, there is a consistent improvement, reaching accuracy between 85.594% and 84.921%. DA - SHA - 512 exhibits further improvement, with accuracy percentages ranging from 89.252% to 88.579%. PME stands out with a considerable accuracy boost, achieving percentages between 92.910% and 92.237%. However, the most notable performance is observed in the SFO - SLO schema, showcasing remarkable accuracy enhancement across all request levels. From Fig.2, we observe that the accuracy shows a consistent increase from 96.568% to 95.895%, indicating the superior performance of the proposed schema compared to the other evaluated methods. The results collectively suggest that the proposed SFO - SLO schema outperforms existing schemas, offering a more robust and efficient solution for accurate data management in cloud environments.

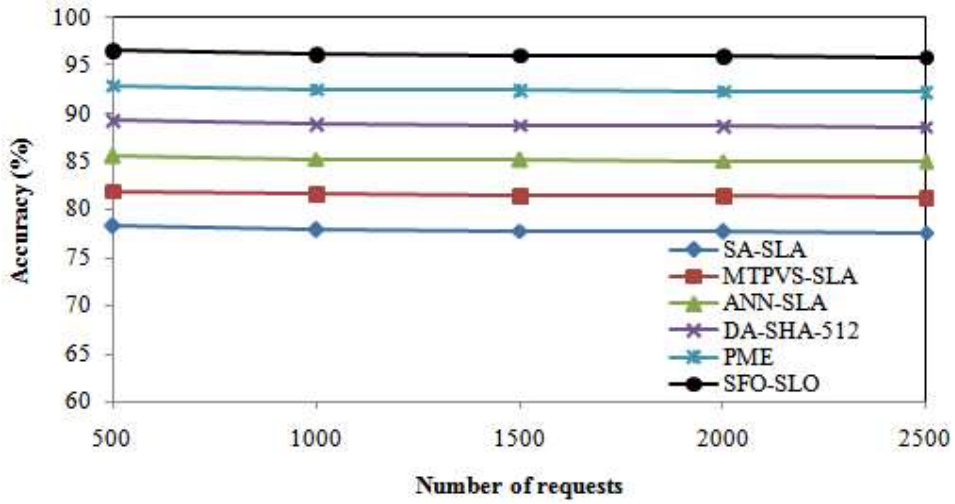

Figure 2: Accuracy comparison for intelligent optimal schemas for vast sensitive data management

Table 2 provides a detailed comparison of precision across different schemas, considering varying numbers of requests. Analyzing the precision metrics, SA - SLA demonstrates values ranging from 76.385% to 75.610% as the number of requests increases. MTPVS - SLA exhibits a slightly higher precision, with values fluctuating between 80.487% and 79.712%. Moving on to ANN - SLA, a consistent improvement is observed, achieving precision percentages between 84.589% and 83.814%. DA - SHA - 512 presents further improvement, with precision values ranging from 88.691% to 87.916%. PME showcases a substantial precision boost, achieving percentages between 92.793% and 92.018%. The most noteworthy enhancement in precision is observed in the SFO - SLO schema, showing a consistent increase from 96.895% to 96.120% across all request levels. it increase underscores the superior precision achieved by the proposed SFO - SLO schema compared to other evaluated methods. The results collectively suggest that the SFO - SLO schema excels in precise data management in cloud like in Fig.3, surpassing the precision performance of existing schemas.

Table 2: Precision comparison

Schemas	Number of requests				
	500	1000	1500	2000	2500
SA - SLA	76.385	76.037	75.891	75.748	75.610
MTPVS - SLA	80.487	80.139	79.993	79.850	79.712
ANN - SLA	84.589	84.241	84.095	83.952	83.814
DA - SHA - 512	88.691	88.343	88.197	88.054	87.916
PME	92.793	92.445	92.299	92.156	92.018
SFO - SLO	96.895	96.547	96.401	96.258	96.120

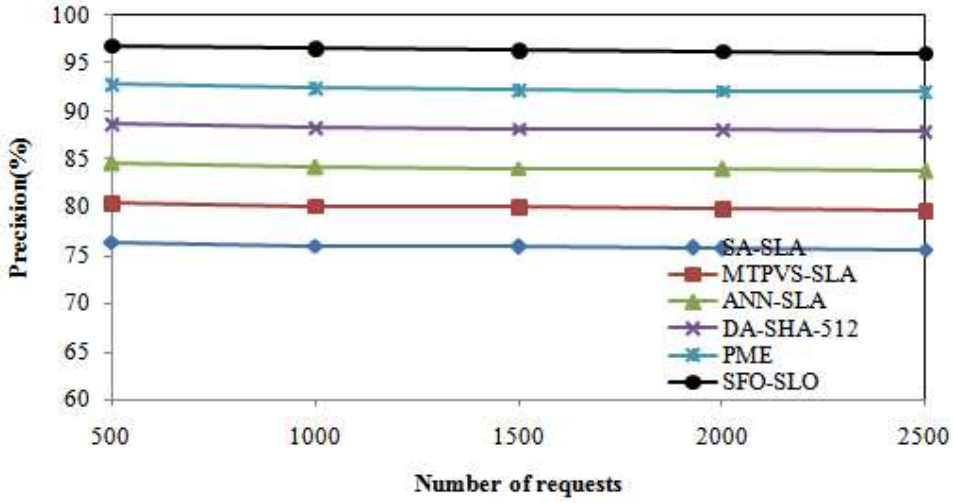

Figure 3: Precision comparison for intelligent optimal schemas for vast sensitive data management

Table 3 outlines a comprehensive comparison of recall metrics for various schemas, considering different numbers of requests. Evaluating the recall performance, SA - SLA exhibits values ranging from 74.948% to 74.247% as the number of requests increases. MTPVS - SLA presents a slightly improved recall, with values fluctuating between 79.183% and 78.482%. ANN - SLA showcases consistent improvement, achieving recall percentages between 83.418% and 82.717%. DA - SHA - 512 further enhances recall, with values ranging from 87.653% to 86.952%. PME demonstrates a significant boost in recall, achieving percentages between 91.888% and 91.187%. The most notable improvement in recall is evident in the SFO - SLO schema, consistently increasing from 96.123% to 95.422% across all request levels. This improvement underscores the superior recall achieved by the proposed SFO - SLO schema compared to other evaluated methods. As shown in Fig.4, results collectively suggest that the SFO - SLO schema excels in providing a robust mechanism for recalling relevant information, surpassing the recall performance of existing schemas.

Table 3: Recall comparison

Schemas	Number of requests				
	500	1000	1500	2000	2500
SA - SLA	74.948	74.839	74.779	74.472	74.247
MTPVS - SLA	79.183	79.074	79.014	78.707	78.482
ANN - SLA	83.418	83.309	83.249	82.942	82.717
DA - SHA - 512	87.653	87.544	87.484	87.177	86.952
PME	91.888	91.779	91.719	91.412	91.187
SFO - SLO	96.123	96.014	95.954	95.647	95.422

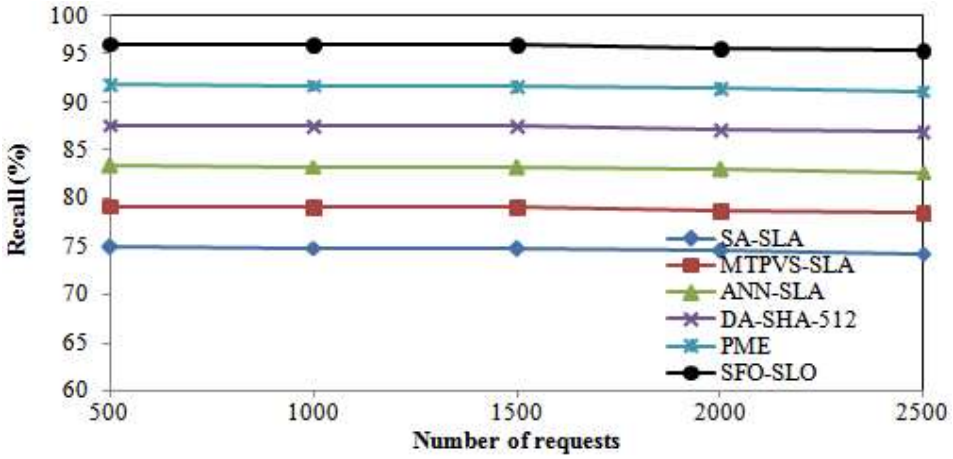

Figure 4: Recall comparison for intelligent optimal schemas for vast sensitive data management

Table 4: Specificity comparison

Schemas	Number of requests				
	500	1000	1500	2000	2500
SA - SLA	81.227	81.026	80.797	80.685	80.564
MTPVS - SLA	84.352	84.151	83.922	83.810	83.689
ANN - SLA	87.477	87.276	87.047	86.935	86.814
DA - SHA - 512	90.602	90.401	90.172	90.060	89.939
PME	93.727	93.526	93.297	93.185	93.064
SFO - SLO	96.852	96.651	96.422	96.310	96.189

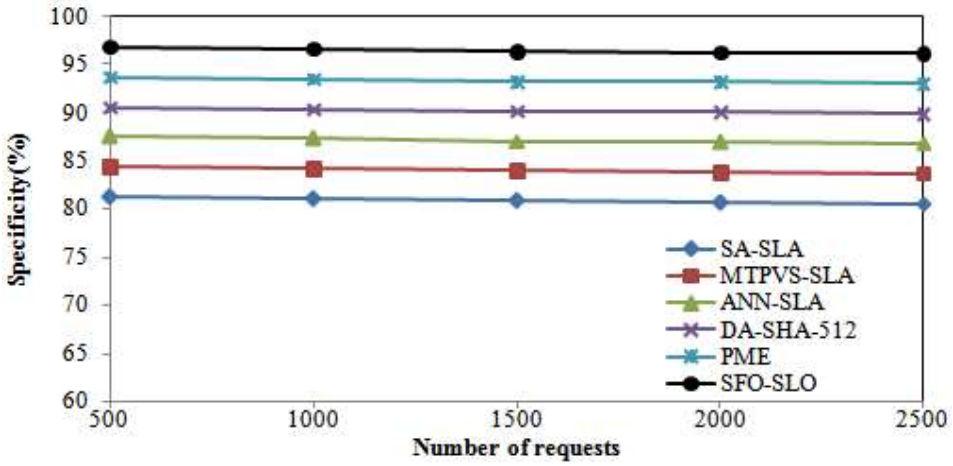

Figure 5: Specificity comparison for intelligent optimal schemas for vast sensitive data management

Table 4 presents a detailed analysis of specificity metrics for different schemas, considering varying numbers of requests. When examining specificity, SA - SLA exhibits values ranging from 81.227% to 80.564% as the number of requests increases. MTPVS - SLA shows consistent improvement in specificity, with values fluctuating between 84.352% and 83.689%. ANN - SLA demonstrates a similar increasing trend, achieving specificity between 87.477% and 86.814%. DA - SHA - 512 further enhances specificity, with values ranging from 90.602% to 89.939%. PME exhibits a notable boost in specificity, achieving between 93.727% and 93.064%. The most remarkable enhancement in specificity is observed in the SFO - SLO schema, consistently increasing from 96.852% to 96.189% across all request levels. This improvement highlights the superior specificity achieved by the proposed SFO - SLO schema compared to other evaluated methods. From Fig.5, we found that outcomes collectively suggest that the SFO - SLO schema excels in providing robust mechanism for optimizing the cloud central server and implementing optimal access control mechanisms.

Table 5: F - measure comparison

Schemas	Number of requests				
	500	1000	1500	2000	2500
SA - SLA	75.660	75.433	75.331	75.105	74.922
MTPVS - SLA	79.830	79.603	79.500	79.274	79.092
ANN - SLA	83.999	83.772	83.670	83.444	83.262
DA - SHA - 512	88.169	87.942	87.839	87.613	87.431
PME	92.338	92.111	92.008	91.782	91.601
SFO - SLO	96.507	96.280	96.177	95.952	95.770

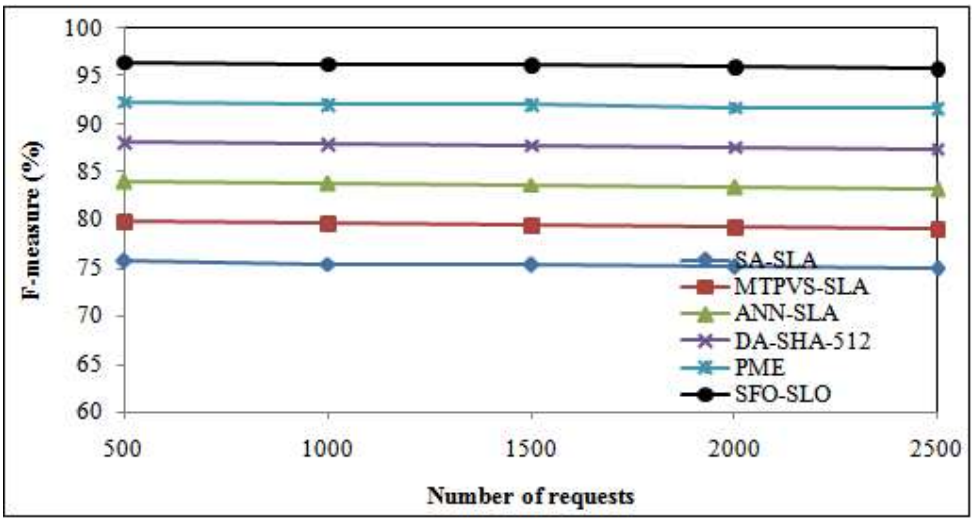

Figure 6: F - measure comparison for intelligent optimal schemas for vast sensitive data management

Table 5 presents a detailed comparison of F - measure metrics for various schemas, considering different numbers of requests. Analyzing the F - measure values, SA - SLA demonstrates a gradual decrease from 75.660% to 74.922% as the number of requests increases. In contrast, MTPVS - SLA exhibits consistent improvement in F - measure, showing an upward trend from 79.830% to 79.092%. Similarly, ANN - SLA experiences a marginal decrease from 83.999% to 83.262%, while DA - SHA - 512 maintains a relatively stable performance, with values fluctuating between 88.169% and 87.431%. PME shows a slight decrease in F - measure, ranging from 92.338% to 91.601%. Remarkably, the most significant increase in F - measure is observed in the SFO - SLO schema, consistently improving from 96.507% to 95.770% across all request levels. This improvement underscores the superior F - measure achieved

by the proposed SFO - SLO schema compared to other evaluated methodologies. Fig.6 indicates that the SFO - SLO schema excels in optimizing the cloud central server and implementing optimal access control mechanisms, leading to a highly effective management of vast sensitive data in cloud environments.

Table 6: Total processing time (ms) comparison

Schemas	Number of requests				
	500	1000	1500	2000	2500
SA - SLA	1960	2248	2581	2716	2738
MTPVS - SLA	1815	2103	2436	2571	2593
ANN - SLA	1670	1958	2291	2426	2448
DA - SHA - 512	1525	1813	2146	2281	2303
PME	1380	1668	2001	2136	2158
SFO - SLO	1235	1523	1856	1991	2013

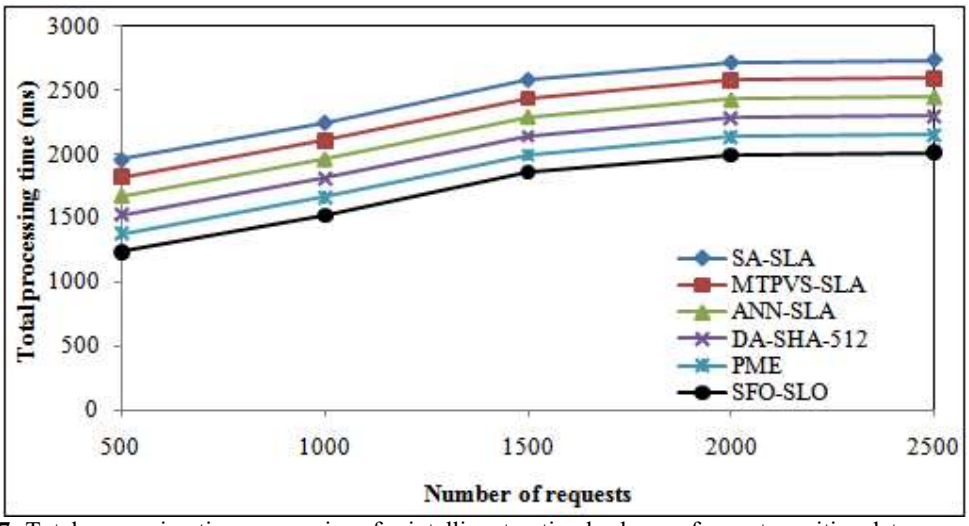

Figure 7: Total processing time comparison for intelligent optimal schemas for vast sensitive data management

Table 6 provides a comprehensive comparison of the total processing time for different schemas, considering varying numbers of requests. Analyzing the results, SA - SLA exhibits an upward trend in total processing time, increasing from 1960 ms to 2738 ms as the number of requests escalates. In contrast, MTPVS - SLA demonstrates a consistent decrease in processing time, showing values ranging from 1815 ms to 2593 ms. Similarly, ANN - SLA experiences a gradual increase from 1670 ms to 2448 ms, while DA - SHA - 512 displays a notable decrease from 1525 ms to 2303 ms. PME shows a continuous reduction in processing time, with values decreasing from 1380 ms to 2158 ms. Notably, the most significant decrease in total processing time is observed in the SFO - SLO schema, consistently decreasing from 1235 ms to 2013 ms across all request levels. Fig.7 shows the decrement emphasizes the superior efficiency of the proposed SFO - SLO schema in optimizing the cloud central server and implementing optimal access control mechanisms.

5. Conclusion

We have introduced an intelligent optimal schema that harnesses the power of soft computing models for the classifying and managing vast sensitive data within cloud environments. The cornerstone of our approach is the smart flower optimization (SFO) algorithm, meticulously crafted to optimize the cloud central server, ensuring system scalability while concurrently reducing user access time and communication delays. To fortify data privacy, we have implemented a time - limited optimal access control mechanism utilizing the snow leopard optimization (SLO) algorithm. The outcomes of extensive performance assessments underscore the prowess of our proposed SFO - SLO schema. The achieved metrics, including an impressive accuracy of 96.16%, precision of 96.44%, recall of 95.83%, and F1 - score of 96.14%, affirm the schema's efficacy in not only enhancing security but also optimizing overall system performance. As the cloud computing landscape continues to evolve, our intelligent optimal schema stands as a robust solution for addressing the intricate challenges associated with managing vast sensitive data securely and efficiently in cloud environments.

References

[1] Van Oosterom, P., Martinez - Rubi, O., Ivanova, M., Horhammer, M., Geringer, D., Ravada, S., Tijssen, T., Kodde, M. and Gonçalves, R., 2015. Massive point cloud data management: Design, implementation and execution of a point cloud benchmark. Computers & Graphics, 49, pp.92 - 125.

[2] Zeng, L., Veeravalli, B. and Zomaya, A. Y., 2015. An integrated task computation and data management scheduling strategy for workflow applications in cloud environments. Journal of Network and Computer Applications, 50, pp.39 - 48.

[3] Arianyan, E., Taheri, H. and Sharifian, S., 2015. Novel energy and SLA efficient resource management heuristics for consolidation of virtual machines in

cloud data centers. Computers & Electrical Engineering, 47, pp.222 - 240.
[4] Castiglione, A., Pizzolante, R., De Santis, A., Carpentieri, B., Castiglione, A. and Palmieri, F., 2015. Cloud - based adaptive compression and secure management services for 3D healthcare data. Future Generation Computer Systems, 43, pp.120 - 134.
[5] Sampaio, A. M., Barbosa, J. G. and Prodan, R., 2015. PIASA: A power and interference aware resource management strategy for heterogeneous workloads in cloud data centers. Simulation Modelling Practice and Theory, 57, pp.142 - 160.
[6] Subbiah, S., Varalakshmi, P., Prarthana, R. and Devi, C. R., 2015. Energy efficient big data infrastructure management in geo - federated cloud data centers. Procedia Computer Science, 58, pp.151 - 157.
[7] Li, K., 2016. Power and performance management for parallel computations in clouds and data centers. Journal of Computer and System Sciences, 82 (2), pp.174 - 190.
[8] Ogiela, L., 2015. Intelligent techniques for secure financial management in cloud computing. Electronic commerce research and applications, 14 (6), pp.456 - 464.
[9] Xing, K., Qian, W. and Zaman, A. U., 2016. Development of a cloud - based platform for footprint assessment in green supply chain management. Journal of cleaner production, 139, pp.191 - 203.
[10] Kouatli, I., 2016. Managing cloud computing environment: Gaining customer trust with security and ethical management. Procedia Computer Science, 91, pp.412 - 421.
[11] Xu, Z., Mei, L., Liu, Y., Hu, C. and Chen, L., 2016. Semantic enhanced cloud environment for surveillance data management using video structural description. Computing, 98, pp.35 - 54.
[12] Jiang, F. and Leung, C. K., 2015. A data analytic algorithm for managing, querying, and processing uncertain big data in cloud environments. Algorithms, 8 (4), pp.1175 - 1194.
[13] Noor, T. H., Sheng, Q. Z., Yao, L., Dustdar, S. and Ngu, A. H., 2015. CloudArmor: Supporting reputation - based trust management for cloud services. IEEE transactions on parallel and distributed systems, 27 (2), pp.367 - 380.
[14] Xia, Z., Wang, X., Sun, X. and Wang, Q., 2015. A secure and dynamic multi - keyword ranked search scheme over encrypted cloud data. IEEE transactions on parallel and distributed systems, 27 (2), pp.340 - 352.
[15] Meharwade, A. and Patil, G. A., 2016. Efficient keyword search over encrypted cloud data. Procedia Computer Science, 78, pp.139 - 145.
[16] Malhotra, S., Doja, M. N., Alam, B. and Alam, M., 2016. Cloud Database Management System security challenges and solutions: an analysis. CSI transactions on ICT, 4, pp.199 - 207.
[17] Rajabzadeh, M. and Haghighat, A. T., 2017. Energy - aware framework with Markov chain - based parallel simulated annealing algorithm for dynamic management of virtual machines in cloud data centers. The Journal of Supercomputing, 73, pp.2001 - 2017.
[18] Arianyan, E., Taheri, H. and Sharifian, S., 2016. Novel heuristics for consolidation of virtual machines in cloud data centers using multi - criteria resource management solutions. The Journal of Supercomputing, 72, pp.688 - 717.
[19] Raza, N., Rashid, I. and Awan, F. A., 2017. Security and management framework for an organization operating in cloud environment. Annals of Telecommunications, 72, pp.325 - 333.
[20] NgnieSighom, J. R., Zhang, P. and You, L., 2017. Security enhancement for data migration in the cloud. Future Internet, 9 (3), p.23.
[21] Moghaddam, F. F., Wieder, P. and Yahyapour, R., 2017. Policy Management Engine (PME): A policy - based schema to classify and manage sensitive data in cloud storages. Journal of information security and applications, 36, pp.11 - 19.