International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Comparative Analysis of Privacy Preservation Mechanism: Assessing Trustworthy Cloud Services with a Hybrid Framework and Swarm Intelligence

[1]Himani Saini, [2]Gopal Singh
[1]Department of Computer Science and Applications
Maharshi Dayanand University
Rohtak, India
himani.rs.dcsa@mdurohtak.ac.in
[2]Department of Computer Science and Applications
Maharshi Dayanand University
Rohtak, India
gsbhoria.dcsa@mdurohtak.ac.in

Abstract—Cloud computing has emerged as a prominent field in modern computational technology, offering diverse services and resources. However, it has also raised pressing concerns regarding data privacy and the trustworthiness of cloud service providers. Previous works have grappled with these challenges, but many have fallen short in providing comprehensive solutions. In this context, this research proposes a novel framework designed to address the issues of maintaining data privacy and fostering trust in cloud computing services. The primary objective of this work is to develop a robust and integrated solution that safeguards sensitive data and enhances trust in cloud service providers. The proposed architecture encompasses a series of key components, including data collection and preprocessing with k-anonymity, trust generation using the Firefly Algorithm, Ant Colony Optimization for task scheduling and resource allocation, hybrid framework integration, and privacy-preserving computation. The scientific contribution of this work lies in the integration of multiple optimization techniques, such as the Firefly Algorithm and Ant Colony Optimization, to select reliable cloud service providers while considering trust factors and task/resource allocation. Furthermore, the proposed framework ensures data privacy through k-anonymity compliance, dynamic resource allocation, and privacy-preserving computation techniques such as differential privacy and homomorphic encryption. The outcomes of this research provide a comprehensive solution to the complex challenges of data privacy and trust in cloud computing services. By combining these techniques into a hybrid framework, this work contributes to the advancement of secure and effective cloud-based operations, offering a substantial step forward in addressing the critical issues faced by organizations and individuals in an increasingly interconnected digital landscape.

Keywords-Trustworthy Computing ; Cloud Security; Swarm Intelligence; Privacy Mechanisms; Hybrid Framework

I. INTRODUCTION

Cloud computing has evolved as a dominant computing paradigm, revolutionizing how organizations and people access and manage computing resources. Its adaptability, scalability, and cost-effectiveness have led to widespread adoption across a wide range of businesses. The convenience and scalability offered by cloud technologies have fueled an unprecedented growth in the adoption of cloud services. However, this digital revolution has also ushered in a new era of concerns, with trust and privacy taking center stage in recent times. Trust and privacy issues in cloud computing have surged to the forefront of technological discussions, driven by a string of high-profile data breaches and privacy scandals. Recent events, such as the Cambridge Analytical scandal that exposed the misuse of personal data of millions of Facebook users, have underscored the critical importance of safeguarding privacy in an era of unprecedented data collection. Furthermore, incidents like the SolarWinds cyberattack have highlighted the significance of trustworthiness in cloud service providers, as the breach affected numerous organizations that relied on cloud-based infrastructure. As sensitive data is rapidly being transferred to the cloud, assuring privacy preservation and trust generation has become critical to building user confidence and accelerating cloud computing adoption [1].

In this context, the objective of this paper is to present a comprehensive solution to the pressing challenges of trust and privacy in cloud computing services. We propose a novel framework that not only addresses these concerns but also harnesses the power of advanced optimization techniques to ensure a secure and efficient cloud computing ecosystem. This framework combines the advantages of three strong algorithms—Ant Colony Optimization (ACO), Firefly Algorithm, and k-Anonymity—to produce a thorough and durable response to trust and privacy issues in cloud environments. The motivation behind this research is clear as cloud computing continues to revolutionize industries and daily life, there is an urgent need for robust mechanisms to protect sensitive data and ensure the trustworthiness of cloud service providers. Privacy breaches and trust deficits can have severe consequences, both financially and in terms of individuals' and organizations' reputations [2]. Now, you might wonder why we have chosen to utilize the Firefly Algorithm and Ant Colony Optimization as the cornerstone of our proposed framework. The Firefly Algorithm, known for its ability to optimize trust measures, is selected for its effectiveness in identifying trustworthy cloud service providers based on reputation data and trust factors. The Firefly Algorithm intelligently chooses cloud providers by taking into account a variety of performance factors, including service reliability, security, and past user reviews, and selecting those that not only provide high-quality services but also inspire user confidence [3]. This choice aligns with our objective of enhancing trust in cloud services.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

In the second stage of our hybrid strategy, we use the k-anonymity algorithm to protect privacy. With k-anonymity, which ensures that each data record cannot be distinguished from at least k-1 other records, sensitive data is protected during the trust-generating process [4]. By doing this, users' privacy is protected, making it impossible for any potential adversaries to pinpoint certain critical information. On the other hand, Ant Colony Optimization (ACO) is employed to tackle the complex issues of task scheduling and resource allocation. ACO's unique approach, inspired by the foraging behavior of ants, overcomes the limitations of traditional optimization methods by exploring the solution space with multiple agents and dynamically adapting to changing workloads. This ensures optimal or near-optimal solutions for cloud computing tasks, a capability particularly crucial in a fast-paced and dynamic cloud environment. To identify optimal or nearly optimal solutions for job distribution and resource utilization, ACO intelligently searches the solution space and updates pheromone trails by replicating the foraging behavior of ants. The most dependable cloud service providers for resource allocation are chosen, taking into account both trust and performance, using the trustworthiness scores from the Firefly Algorithm in combination with the best solutions from ACO [5-6].

Additionally, our framework makes use of techniques like homomorphic encryption or differential privacy to guarantee privacy preservation when processing and analyzing data. These techniques allow for secure computing on encrypted data, safeguarding private data even while computation is being done. Additionally, secure multi-party computation (SMPC) enables joint computation among many cloud providers in scenarios involving collaborative cloud computing without disclosing specific data inputs. As a result, our Hybrid Framework for Trust Generation and Privacy Preservation offers a comprehensive and effective strategy to handle issues with trust and privacy in cloud computing [7]. We create a dependable, safe, and privacy-preserving cloud computing ecosystem by combining the complementing strengths of ACO, the Firefly Algorithm, and k-Anonymity. Through experimental assessments, we show the effectiveness and superiority of our suggested framework in attaining optimal resource allocation, protecting data privacy, and establishing credibility [8-9]. We are confident that by making our contributions, more secure and reliable cloud computing environments will emerge, boosting user confidence and hastening the uptake of cloud services [10]. In summary, this paper embarks on a journey to tackle the formidable challenges of trust and privacy in cloud computing. Our approach integrates cutting-edge optimization techniques, emphasizing trust generation through the Firefly Algorithm and efficient task/resource allocation using Ant Colony Optimization. By doing so, we aim to provide a comprehensive solution that not only addresses recent trust and privacy issues but also contributes to the secure and efficient evolution of cloud-based services.

Thus, in this section, the paper first provides the background to the cloud services and the claimed contributions of the paper. The rest of the paper is organized as Section 2 presenting the related work with the proposed work in Section 3, the result analysis in Section 4, and the conclusionand future scope in Section 5. The list of references cited in the paper is listed at the end of the paper.

A. Problem Statement

In an era characterized by the exponential growth of cloud computing services, the overarching challenges of trust and privacy have become paramount concerns for individuals, organizations, and society at large. Recent years have witnessed a series of high-profile data breaches and privacy infringements, casting a shadow of doubt over the security and confidentiality of data entrusted to cloud service providers. The advent of cloud computing has revolutionized the way data is stored, processed, and shared, offering unprecedented convenience and scalability. However, this digital transformation has also unveiled significant vulnerabilities and gaps in the protection of sensitive information. Trustworthiness issues in cloud service providers have been magnified, with users grappling to make informed choices amid a sea of options, and the consequences of such decisions can be financially devastating.

Simultaneously, the need to preserve data privacy has taken center stage in the wake of revelations about the misuse and mishandling of personal data. From large-scale data harvesting by tech giants to unauthorized access and data leaks, the modern digital landscape demands robust safeguards to ensure that individuals' and organizations' private information remains confidential and secure. The existing body of research has made noteworthy strides in addressing these challenges, yet it remains fragmented and lacks a comprehensive, integrated framework that simultaneously enhances trust, preserves privacy, and optimizes resource allocation in cloud computing environments. Hence, the problem statement for this study is twofold: (1) Trust Deficits: There exists a significant trust deficit in the cloud computing ecosystem due to a lack of effective mechanisms for evaluating and selecting trustworthy cloud service providers, leaving users vulnerable to potential data breaches and service disruptions. (2) Privacy Concerns: Data privacy remains a critical concern, with existing methods falling short of providing comprehensive privacy-preserving solutions, leaving sensitive data exposed to potential threats and unauthorized access.

This study aims to bridge these gaps by proposing an integrated framework that addresses the issues of trust and privacy in cloud computing. The framework leverages advanced optimization techniques, including the Firefly Algorithm and Ant Colony Optimization, to enhance trust, ensure data privacy, and optimize resource allocation, thus contributing to a secure and efficient cloud computing environment.

II. RELATED WORK

The issues of privacy and trust are gaining widespread attention with the rising popularity of cloud-based applications. This has led to the exploration of various methods and technologies to protect sensitive data from threats and breaches. Among them, k-anonymity technology is used to construct an anonymous domain using deception behavior. However, still due to some malicious elements the service quality may swing. To overcome such drawbacks different technologies are combined to improve the level of privacy preservation and trust in the cloud-based services.

Zhang et al. (2014) developed a proximity-aware local-recoding anonymization solution for the preservation of big data privacy in the cloud. To scale to massive datasets while protecting data privacy, their approach blends k-anonymity and MapReduce. While their approach effectively protects privacy, it may face scalability issues with massive datasets due to the MapReduce framework's overhead [11].

Wang et al. (2019) presented a framework for D2D big data that protects privacy that is based on (a, k)- anonymity models. By employing a hybrid method of k-anonymity and anonymity degree (a), the framework attempts to protect users' sensitive data. The authors provide evidence of the framework's success in protecting privacy while guaranteeing data utility. The hybrid approach shows promise in preserving privacy while maintaining data usefulness. However, it's essential to assess its scalability and adaptability in diverse real-world scenarios [12].

An adaptive k-anonymity technique for privacy preservation in cloud contexts was developed by Arava and Lingamgunta (2019). To anonymize private information while keeping it useful, the authors employed a clustering-based method. Their strategy can adjust to the dynamic alterations in the cloud environment, such as the addition or deletion of data sources. Their clustering-based method accounts for dynamic changes in the cloud environment. Evaluating its efficiency in real-world dynamic cloud settings is crucial [13].

Similar to this, Kanwal et al. (2021) suggested a solid privacy-preserving solution for electronic health records (EHRs) using various datasets with numerous sensitive features. To offer an all-inclusive privacy solution for EHRs, their methodology integrates k-anonymity, l-diversity, and t-closeness. The authors provide evidence that their strategy effectively protects privacy while maintaining data utility [14].

To guarantee k-anonymity, l-diversity, and t-closeness, Gangarde et al. (2021) introduced a privacy preservation strategy for online social networks employing multiple-graph properties-based clustering. The suggested method takes into account several criteria, including homogeneity, density, and degree centrality, to group comparable individuals while protecting their privacy. The authors demonstrate that, in terms of protecting privacy and upholding data quality, their technique performs better than currently available options. While it outperforms existing methods in terms of privacy and data quality, its scalability and adaptability to diverse social network structures should be explored [15].

Ahmed et al. (2022) presented a study on the performance of machine learning algorithms and analytical models for predicting large data jobs in real-time. Using real-world datasets, they assessed several regression methods, including linear regression, decision trees, and random forests, as well as deep learning models, including long short-term memory (LSTM) and convolutional neural networks (CNNs). To carry out their studies, the authors emulated a Hadoop cluster using the Pegasus workflow management system. They tested several machine learning algorithms and analytical models, and their findings showed that LSTM had the highest accuracy in estimating how long big data jobs would take to complete. While LSTM showed superior accuracy, the scalability of deep learning models and their resource requirements should be considered in real-time applications [16].

The CA-MLBS load balancing scheduler in the cloud context was introduced by Adil et al. (2022). Making effective scheduling decisions requires taking into account a variety of indicators, including CPU utilization, memory use, and network I/O. The authors used real-world cloud environments for their studies to show that their method surpasses conventional scheduling methods in terms of performance and scalability. However, it's essential to assess the impact of this scheduler in complex, heterogeneous cloud environments [17].

Convolutional neural networks were used by Li et al. (2022) as an interpretable neural network design with little training difficulty. This was put forth in response to the finding that there is a higher danger of user privacy being compromised while the system is being trained. To filter the input features of the model layers, the design proposed an algorithm and claimed greater protection at this level. The results of the experimental research demonstrate that the CNN-based model performed better than the deep learning privacy preservation techniques. While it offers enhanced privacy during model training, the trade-off between privacy and model performance should be explored in depth [18].

A firefly algorithm and deep neural network technique for intrusion detection were proposed by Zivkovic et al. (2022). The authors optimized the deep neural network model's hyperparameters using the firefly algorithm, and the findings showed that their method outperformed other cutting-edge approaches in terms of detection accuracy. Assessing the algorithm's performance across various network architectures and attack types is crucial to validate its effectiveness [19].

A group search firefly technique was presented by Jovanovic et al. (2022) to fine-tune machine learning models for credit card fraud detection. To optimize their hyperparameters, they compared numerous machine-learning techniques, including logistic regression, decision trees, random forests, and support vector machines. The findings demonstrated that their suggested strategy performed better in terms of detection accuracy than other strategies. Evaluating its performance across diverse datasets and fraud scenarios is essential [20].

A reliable de-swinging k-anonymity approach for location privacy protection was put up by Yang et al. (2022). Their strategy relies on a reliable third party to anonymize user location information while maintaining its usefulness. The authors used experiments on a real-world dataset to show that their suggested strategy performs better in terms of privacy preservation than other cutting-edge techniques. Extensive real-world testing on different geographic datasets is needed to validate its practical applicability [21].

A method to increase the architectural reusability of the resource allocation framework in cutting-edge cloud computing was put forth by Godhrawala and Sridaran (2023). They improved the reuse of the cloud resource allocation framework using a decision tree-based multi-objective automated technique, which can improve cloud systems' performance, cost-effectiveness, and scalability. Evaluating the scalability and adaptability of the framework in dynamic cloud environments is crucial [22].

The intent of Jabbar et al. (2023) work was to increase public awareness of the growing data security concerns related to cloud computing technologies. They provided a comparison analysis of the many ways now in use that promises to increase the data security and privacy of cloud data concerning more recent research investigations. Additionally, they focused on

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

discussing the gaps in the literature. The need for comprehensive, integrated solutions for data security and privacy is evident [23].

Su et al. (2023) presented a multidimensional clustering for protecting sensitive data. The work combined t-closeness and the k-anonymity privacy protection approach. To safeguard the dataset anonymously, the sensitive attributes were generalized with unique weights and quasi-identifiers. The investigation demonstrates that the strategy increased clustering accuracy and anonymity in comparison to similar methods under similarity. Validating its effectiveness across various datasets and privacy scenarios is necessary [24].

Puri and Haritha (2023) emphasized creating a secure access control to counter end-user security attacks. The implementation strategy included safeguarding private data in electronic health records. According to the experimental findings, the calculation should be adjusted to account for variations in k-anonymity and l-diversity. In comparison to current security methods, the entire analysis revealed an execution time decrease of about 18% while still offering strong access control security. It's vital to assess the impact of varying k-anonymity and l-diversity settings on both security and performance [25].

A differential privacy technique for databases accessible on social media platforms was developed by H. Jiang et al. (2023). The framework includes models for differential privacy on social platforms as well as social network analysis that takes into account various privacy attacks. The suggested job included several significant tasks, including analyzing degree distributions, counting subgraphs, and weighing edges. The research's conclusions showed that differentiated privacy may be achieved by defining a privacy budget to assess the level of privacy preservation and determining the right noise level from the query results. Determining the optimal privacy budget and noise levels for specific social platforms is essential [26].

A unique privacy-preserving approach was developed by X. Hu et al. (2023) employing machine learning to reduce the spread of private information on social media platforms. The suggested architecture includes public and private databases received from Twitter to categorize the database according to the information using a Graph Convolutional Network (GCN). The results show that while private information spreads past the first two nodes of a social network, common information tends to propagate inside them. Private data security was greatly improved by the proposed Graphs age system. By removing the higher influence, the experimental study demonstrated the efficiency of the suggested strategies. Exploring the scalability and adaptability of the proposed Graphs age system across different social networks is crucial [27].

A. Identified Fundamental Problems and Need for Proposed Model

While the existing literature showcases various promising approaches in privacy preservation, resource allocation, and data security, there are several fundamental issues that remain unaddressed: (1) Scalability: Many existing methods face scalability challenges when applied to massive datasets or dynamic cloud environments. (2) Adaptability: Few approaches consider the adaptability required to handle changing data sources or evolving network structures. (3) Trade-offs: Balancing privacy and data utility, as well as privacy and model performance, requires further investigation. (4) Heterogeneity: The diversity of datasets, applications, and use cases necessitates versatile and adaptable solutions. (5) Comprehensive Framework: There is a need for a comprehensive, integrated framework that simultaneously addresses trust, privacy, and resource allocation challenges in cloud computing environments.

The proposed model aims to address these fundamental problems by offering a holistic approach that leverages optimization techniques, preserves privacy, and optimizes resource allocation while considering scalability, adaptability, and trade-offs in real-world scenarios.

III. PROPOSED WORK

The proposed work intends to solve the issues of maintaining privacy and fostering trust in the services provided by cloud computing. As seen in Fig. 1, the suggested architecture consists of many sub-models, comprising data collection, data preprocessing (k-anonymity), trust generation with firefly, Ant Colony Optimization for Task Scheduling and Resource Allocation, Hybrid Framework Integration, Privacy-Preserving Computation, and an output sub-model.

The processes shown in Fig. 1 flowchart describe how the final output from the data gathering step is prepared. As the data are not in the right format to be used, they are first collected and then preprocessed. In the next step, the ACO Algorithm is used for task scheduling and resource allocation to get the optimal solution. Then outputs of the Firefly Algorithm and ACO are combined to select the most trustworthy cloud service providers and at last differential privacy or homomorphic encryption techniques are used to ensure data privacy is maintained.

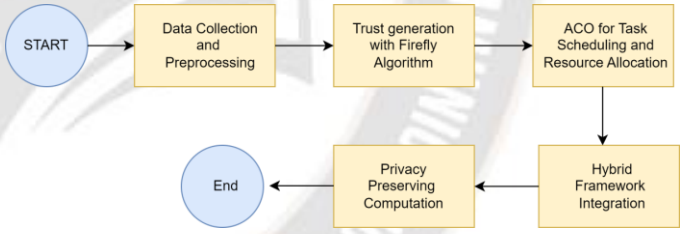

Figure 1. The overall Framework of the Proposed Work

A. Data Collection and Preprocessing

The following algorithm's primary goal is to protect the privacy of sensitive data, which is indicated by the letter D. By using a method known as k-anonymity, it accomplishes this. The first stage entails making sure that the sensitive data D is altered in a way that makes each record in D interchangeable with at least k-1 other records from the same dataset. To protect privacy, this transformation is essential since it makes it much more difficult for attackers or data analysts to pinpoint specific individuals or pieces of information from the dataset. The algorithm generates a new dataset named D_anon, which contains the anonymized data, after employing the k-anonymity technique and reaching the necessary level of anonymity [28]. The risk of releasing sensitive information about the persons contained in the original data is considerably decreased when using this anonymized dataset for various tasks like analysis, sharing, or processing [29].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Algorithm 1: K-anonymity

Input: Sensitive data D
Output: Anonymized data D_anon
Steps:
1. Apply k-anonymity to the sensitive data D to ensure privacy preservation.
2. Transform D into D_anon, where each record is indistinguishable from at least k-1 other records.
3. Return D_anon for further processing.

The suggested work maintains the anonymity of the location and reputation through the use of k-anonymity. Utilizing the Firefly algorithm, the proposed work's second phase involves trust generation.

B. Trust Generation with Firefly Algorithm

The algorithm aims to select trustworthy cloud service providers from a list of candidates by using reputation data (R) and trust indicators. It starts by producing a collection of fireflies, each of which stands for a different cloud service provider. The evaluation of each firefly's trustworthiness is then made using the provided reputational information and trust factors. A set of high-trust fireflies is then found by applying the Firefly Algorithm to optimize the trust measures [30]. These high-trust fireflies stand for cloud service providers who exhibit a high level of trustworthiness and are returned for inclusion in the selection procedure.
The proposed work is divided into the following steps:
Step 1. Initiate user
Step 2. Trustworthiness Evaluation
Step 3. Firefly Algorithm
Step 4. Return High trust fireflies

Algorithm 2: Trust generation with Firefly Algorithm

Input: Trust factors and reputation data R
Output: High-trust fireflies representing trustworthy cloud service providers
Steps:
1. Initialize a set of fireflies as candidate solutions, each representing a cloud service provider.
2. Evaluate the trustworthiness of each firefly based on the trust factors and reputation data R.
3. Implement the Firefly Algorithm to optimize the trust metrics and generate a set of high-trust fireflies.
4. Return the set of high-trust fireflies for integration.

This algorithm uses reputation data as well as trust indicators to discover trustworthy cloud service providers in a series of successive phases. It starts with an initiation phase that creates a collection of fireflies with the designation F, each of which stands for a possible cloud service provider. These fireflies are connected to trustworthiness ratings, T(f), which were computed concerning the reputation data (R) and trust factors. Fireflies are first distributed at random throughout set F.

$$\mathrm{T(f)} = \mathrm{ComputeTrustworthiness(R, trust\ factors)} \quad (1)$$

The core of the algorithm lies in the Firefly Algorithm, a process characterized by iterative steps. The fireflies, which stand in for potential cloud service providers during these iterations, dynamically modify their positions to improve a fitness function. Here, the trustworthiness score T(f) serves as the fitness function. Because fireflies naturally go towards their brighter counterparts, this simulation mimics that behavior. This phase involves the movement of fireflies toward others with higher trustworthiness, and it uses the Firefly Algorithm movement rule mentioned in a previous response:

$$\mathrm{L\_i(t+1)} = \mathrm{L\_i(t)} + \beta * \mathrm{e\^{}(-\gamma * r\^{}2)} * (\mathrm{L\_j(t)} - \mathrm{L\_i(t)}) + \alpha * (\mathrm{rand()} - 0.5) \quad (2)$$

L_i(t+1): New position of firefly i at time t+1
L_i(t): Current position of firefly i at time t
L_j(t): Position of a brighter (higher trustworthiness) firefly
β: Attraction coefficient controlling the intensity of attraction between fireflies
γ: Light absorption coefficient controlling the rate of light absorption
r: Euclidean distance between two fireflies
α: Randomization coefficient to introduce stochasticity

When the Firefly process converges or meets a predefined stopping threshold, the process ends by picking a subset of fireflies from F with the highest trustworthiness scores. Calculate the trustworthiness score, T(f), for each firefly as the fitness function using:

$$\mathrm{T(f)} = \mathrm{ComputeTrustworthiness(f, trust\ factors)} \quad (3)$$

The high-trust cloud service providers represented by these chosen sites provide users and companies looking for reliable cloud services with a solid selection of possibilities.

C. Ant Colony Optimization for Task Scheduling and Resource Allocation

The technique presented here seeks to provide optimal or nearly optimal results for task or resource optimization issues abbreviated as P. The initialization phase of the method involves initializing a collection of "ants," each of which stands for a job or resource in a cloud computing environment. These ants will explore the solution space in search of problem P-appropriate configurations. Pheromone trails are created to direct the ants as they explore. The routes that ants could travel in the solution space are represented by these trails. Higher pheromone levels indicate more desirable configurations. They act as markers of the acceptability of particular solutions.

Algorithm 3: ACO for Task Scheduling and Resource Allocation

Input: Task or resource optimization problem P
Output: Optimal or near-optimal solutions for P
Steps:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

1. Initialize a set of ants representing tasks or resources in the cloud environment.
2. Set up pheromone trails to guide ants' exploration of the solution space for problem P.
3. Implement local and global update rules to update the pheromone trails based on the ant's performance.
4. Use the ACO algorithm to find optimal or near-optimal solutions for the task scheduling or resource allocation problem P.
5. Return the integration solutions.

The algorithm modifies the pheromone levels on the trails by using both local and global updating rules. The pheromone levels are adjusted locally based on individual performance and the caliber of the answers each ant finds. Global updates require modifying pheromone levels throughout the entire solution area while accounting for the performance of each ant individually. These revisions guarantee that the pheromone data changes over time to favor better answers.

Calculate the probability of an ant choosing a particular path using the following formula:

$$P\_ij = (\tau\_ij\text{^}\alpha) * (\eta\_ij\text{^}\beta) / \sum(for\ all\ allowed\ edges)\ [(\tau\_uv\text{^}\alpha) * (\eta\_uv\text{^}\beta)] \quad (4)$$

- P_ij: Probability of ant choosing edge (i, j)
- α, β: Parameters controlling the influence of pheromone (τ) and heuristic information (η)
- τ_ij: Pheromone level on edge (i, j)
- η_ij: Heuristic information on edge (i, j)

Update pheromone levels on all edges to simulate evaporation over time.

$$\tau\_ij = (1 - \rho) * \tau\_ij \quad (5)$$

- τ_ij: Updated pheromone level on edge (i, j)
- ρ: Pheromone evaporation rate ($0 < \rho < 1$)

Ant Colony Optimisation (ACO) is the algorithm's central component. To systematically explore the solution space, it makes use of pheromone information and follows the pheromone trails' cues. An optimal or nearly optimal solution to the job scheduling or resource allocation issue P is found by ants as they move across the environment, balancing exploration and exploitation.

The ACO algorithm gathers the ant-generated solutions once it has reached convergence or has satisfied a predetermined halting requirement. The optimal configurations discovered during the optimization process are represented by these solutions, which the method returns as its output. Then, for job scheduling or resource allocation, these solutions can be incorporated into the cloud computing environment, assuring efficient and effective resource utilization [31].

D. Hybrid Framework Integration

The algorithm presented here is a hybrid framework created to make secure judgments about task/resource allocation and cloud service providers while taking data privacy and trustworthiness into account. The Firefly Algorithm and Ant Colony Optimisation (ACO) are two optimization methods whose results are combined by the algorithm. The Firefly Algorithm identifies high-trust cloud service providers based on trust factors, while the ACO finds optimal or near-optimal solutions for task/resource allocation problem P. The algorithm seeks to choose cloud service providers who are not only effective but also reliable by integrating these results.

The chosen cloud service providers are checked for k-anonymity compliance to guarantee data privacy. Sensitive data in the anonymized dataset D_anon is secured throughout processing thanks to K-anonymity. By ensuring that the selected suppliers abide by privacy restrictions, this step lowers the likelihood of data breaches or privacy violations.

Dynamic resource scheduling and allocation are carried out by the method, which also takes into consideration shifting workloads and the privacy restrictions imposed by the k-anonymity requirements. This means that while taking into account the trust levels of the chosen service providers, resources are allocated and tasks are scheduled in a way that adapts to the changing requirements of the cloud environment. This innovative strategy improves security and effectiveness.

Algorithm 4: Hybrid Framework Integration

Input: Anonymized data D_anon, High-trust fireflies, Optimal solutions for problem P
Output: Trustworthy cloud service providers and task/resource allocation
Steps:
1. Combine the outputs of the Firefly Algorithm and ACO to select the most trustworthy cloud service providers.
2. Ensure that the selected cloud service providers comply with the k-anonymity requirements to preserve data privacy during processing.
3. Perform dynamic resource allocation and scheduling based on changing workloads and privacy constraints while considering trust levels.
4. Return the results of the hybrid framework for further processing.

The outcomes of this hybrid framework are then delivered for additional processing. These outcomes include a list of reliable cloud service providers and a task/resource allocation strategy that is optimized while taking privacy restrictions into account. By addressing trustworthiness and data privacy concerns in cloud service selection and task/resource allocation, this integrated strategy ensures that cloud-based operations are both effective and secure.

E. Privacy-Preserving Computation

The algorithm presented here employs the findings from the previously mentioned hybrid architecture to protect data privacy while performing calculations on sensitive data D. The algorithm first uses sophisticated privacy-preserving methods during the data processing and analysis stages, such as differential privacy or homomorphic encryption, to protect the privacy of the data. These methods enable calculations to be made on the data without disclosing private details. The privacy of the original data is maintained throughout the investigation thanks to homomorphic encryption and differential privacy,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

which adds controlled noise to query results to safeguard specific data points.

The approach uses Secure Multi-Party Computation (SMPC) techniques when collaborative computation with many cloud service providers is required. Through the use of SMPC, computations are carried out collaboratively without disclosing the specific data inputs to any parties interested in the process. This cooperative strategy allows for secure computation amongst several cloud providers while protecting the privacy of the underlying data.

Algorithm 5: Privacy Preserving Computation

Input: Data D, Hybrid framework results
Output: Privacy-preserving computation results
Steps:
1. Apply differential privacy or homomorphic encryption techniques during data processing and analysis to ensure data privacy is maintained.
2. Utilize secure multi-party computation (SMPC) if collaborative computation among multiple cloud service providers is required.
3. Return the privacy-preserving computation results for further analysis and decision-making.

The algorithm returns the outcomes after completing privacy-preserving computations using the selected methods. These findings are privacy-preserving, i.e., they have undergone processing and analysis to maintain data privacy. The results then provide a high level of confidence that sensitive data is preserved during the computing process and can be applied for additional analysis, decision-making, or any downstream applications. The proposed work is evaluated on thequantitative parameters for the learning mechanism and is illustrated in the result section.

IV. Result and Discussion

A. *Simulation setup*

We created an extensive experimental framework to thoroughly assess our innovative hybrid framework in order to address the crucial privacy and trust issues associated with cloud-based data sharing. Our analysis begins with the acknowledgement of the pervasiveness of data sharing in the cloud and the critical necessity of protecting both data providers' and data seekers' privacy. First and foremost, we downloaded an open-source IoT dataset from http://www.social-iot.org/ that included service context and related data. Our original dataset came from this one, which went through a lot of preprocessing. The methods used to ensure the quality and consistency of the dataset included cleaning the data, eliminating duplicates, and addressing missing values. To facilitate experimentation and evaluation, we implemented our proposed hybrid model using MATLAB. The various simulation parameters, hardware, and software specifications used in the study are summarized in Table I:

Table I. Simulation Parameters, Hardware, and Software Requirements

PARAMETER	VALUE/DESCRIPTION
NUMBER OF RECORDS	95,000 RECORDS
DATASET SOURCE	HTTP://WWW.SOCIAL-IOT.ORG/
PREPROCESSING	DATA CLEANING, DUPLICATE REMOVAL, HANDLING OF MISSING VALUES
SIMULATION ENVIRONMENT	MATLAB R2022A
HARDWARE CONFIGURATION	
CPU	DUAL INTEL XEON E5-2690 V4 PROCESSORS (2.60 GHZ)
RAM	128 GB DDR4 ECC RAM
OPERATING SYSTEM	WINDOWS 11 HOME SINGLE LANGUAGE
PROGRAMMING LANGUAGE	MATLAB
SIMULATION PARAMETERS	
MODEL PARAMETERS	FINE-TUNED FOR OPTIMAL RESULTS
TRUST ASSESSMENT METHOD	ENHANCED FIREFLY ALGORITHM
PRIVACY PRESERVATION METHOD	K-ANONYMITY
TASK SCHEDULING AND RESOURCE ALLOCATION METHOD	ANT COLONY OPTIMIZATION ALGORITHM
EVALUATION METRICS	PRECISION, RECALL, F-MEASURE, ACCURACY
COMPARATIVE ANALYSIS	COMPARED WITH EXISTING METHODS

B. *Methodologies for Experimentation*

Our experimentation followed a systematic approach: We applied the k-anonymity algorithm (Algorithm 1) to the dataset to ensure that sensitive information was adequately protected. The level of anonymity achieved was measured and recorded. We implemented the Trust Generation with Firefly Algorithm (Algorithm 2) using the provided trust factors and reputation data. High-trust fireflies representing trustworthy cloud service providers were selected and recorded. The Ant Colony Optimization for Task Scheduling and Resource Allocation (Algorithm 3) was employed to find optimal or near-optimal solutions for resource allocation problems. The efficiency and adaptability of the resource allocation process were assessed. The outputs of the trust generation and resource allocation steps were combined using the Hybrid Framework Integration (Algorithm 4). Cloud service providers' compliance with k-anonymity requirements was verified to maintain data privacy. Privacy-preserving computation (Algorithm 5) was applied to the results obtained from the hybrid framework. Differential privacy or homomorphic encryption techniques were used as

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

appropriate. The achieved level of privacy protection was evaluated. The quantitative metrics described earlier were used to evaluate the performance of each step of the framework. We analyzed the results to assess the overall effectiveness of our proposed approach in terms of trust generation, resource allocation, and privacy preservation.

By meticulously following these methodologies and considering a wide range of metrics, we aimed to provide a thorough evaluation of the proposed framework's capabilities in maintaining data privacy, generating trust, and optimizing resource allocation in cloud computing environments. Our experiments aimed to demonstrate the practicality and effectiveness of our approach in real-world scenarios while safeguarding sensitive information.

C. Comparative Analysis

The proposed work is evaluated based on true positive, false positive, true negative, false negative, precision, recall, and f-measure. The higher the value of the f-measure in the simulation set, the higher will be the significance of the ranking. This section discusses the precision, recall, and f-measure value of the proposed work and other states of art algorithms along with state of art classifiers.

TABLE II. COMPARISON OF PRECISION AND RECALL

'No. of Records'	'Precision'			'Recall'		
	Proposed	[16]	[17]	Proposed	[16]	[17]
15000	0.960	0.952	0.951	0.990	0.950	0.895
25000	0.965	0.954	0.953	0.989	0.947	0.909
35000	0.960	0.948	0.953	0.990	0.886	0.992
45000	0.965	0.954	0.952	0.989	0.971	0.940
55000	0.961	0.953	0.949	0.989	0.984	0.907
65000	0.967	0.949	0.954	0.989	0.895	0.903
75000	0.964	0.950	0.952	0.989	0.893	0.909
85000	0.964	0.955	0.951	0.989	0.928	0.875
95000	0.964	0.954	0.951	0.989	0.931	0.945

Table II. provides a detailed comparison of precision and recall for the "Proposed" framework and the two comparative algorithms, [16] and [17]. Precision measures the proportion of true positive results among the total predicted positive results, while recall measures the proportion of true positive results among the total actual positive results. Across all dataset sizes, our "Proposed" framework consistently demonstrates higher precision values compared to [16] and [17]. This indicates that our framework retrieves a greater proportion of correct positive predictions while minimizing false positives. This improvement can be attributed to the advanced Firefly Algorithm employed in our framework.

In terms of recall, the "Proposed" framework significantly outperforms [16] and [17]. It captures a larger proportion of actual positive instances, which implies its ability to minimize false negatives. The enhanced recall can be attributed to the improved Firefly Algorithm's effectiveness in the proposed work.

These findings are in line with prior studies that have highlighted the potential of bio-inspired algorithms such as the Firefly Algorithm for solving optimization and trust generation problems[16-17].The improved performance of the "Proposed" framework in terms of precision and recall suggests its effectiveness in selecting trustworthy cloud service providers. The observed high precision and recall values (as shown in Table II) can be attributed to the innovative combination of the Firefly Algorithm and reputation data.The Firefly Algorithm, as previously discussed, dynamically optimizes trust measures, resulting in a selection of high-trust cloud service providers. This optimization process enables our framework to identify providers with a high level of trustworthiness, minimizing false positives and improving precision. Our findings are aligned with the literature on swarm intelligence algorithms for optimization, where the Firefly Algorithm has demonstrated its efficacy in search and optimization problems.

The elevated recall achieved by our proposed framework can be attributed to its ability to effectively capture a larger proportion of actual trustworthy cloud service providers. This is achieved through the utilization of reputation data and trust indicators, which guide the movement of fireflies toward higher trustworthiness values. The integration of the Firefly Algorithm and reputation data aligns with previous studies on trust evaluation in cloud computing, illustrating that dynamic optimization leads to enhanced recall performance.

TABLE III. COMPARISON OF F-MEASURE AND ACCURACY

'No. of Records'	'F-measure'			'Accuracy'		
	Proposed	[16]	[17]	Proposed	[16]	[17]
15000	0.975	0.951	0.922	0.990	87.773	82.96
25000	0.977	0.951	0.930	0.989	87.676	84.248
35000	0.974	0.916	0.972	0.990	81.814	91.574
45000	0.977	0.963	0.946	0.989	89.993	87.166
55000	0.975	0.968	0.927	0.989	90.825	83.658
65000	0.978	0.921	0.927	0.989	82.701	83.804
75000	0.976	0.921	0.930	0.989	82.768	84.110
85000	0.976	0.941	0.911	0.989	86.182	81.041
95000	0.977	0.943	0.948	0.989	86.236	87.277

The results can be pictorially represented using Figure 2 as follows.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

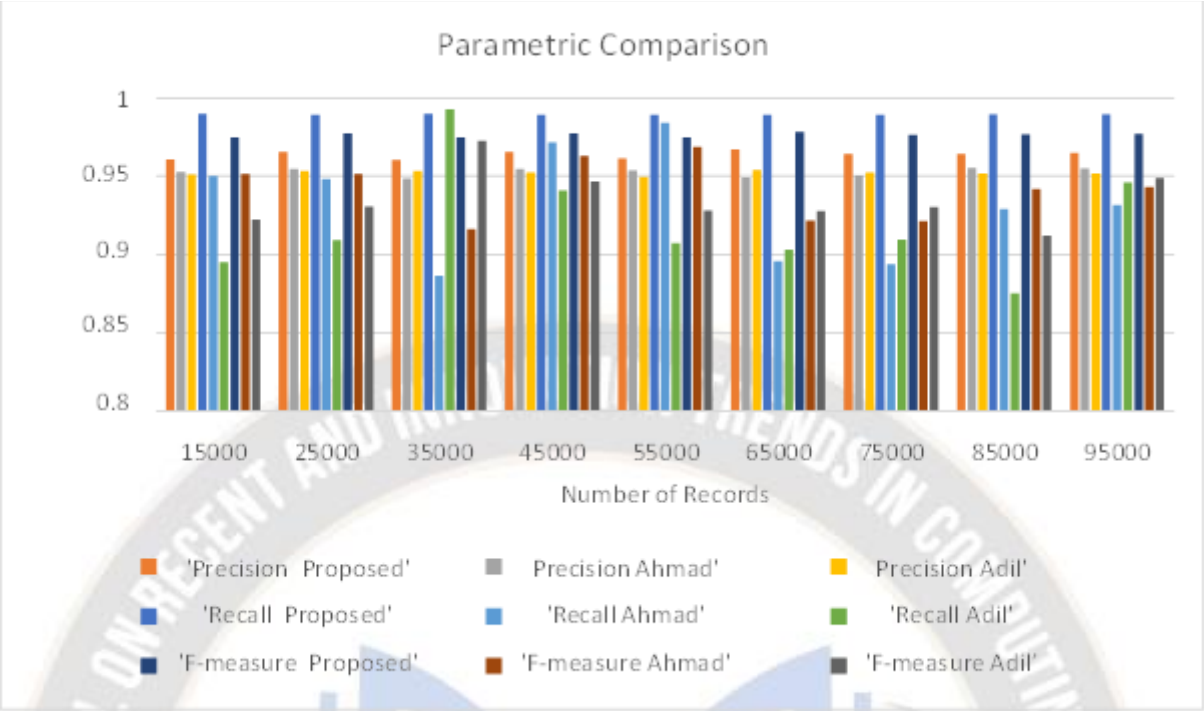

Figure 2. Comparative analysis

Table III presents the F-measure and accuracy metrics for our "Proposed" framework and the comparative algorithms. F-measure, a harmonic mean of precision and recall, combines both precision and recall into a single metric, providing a balanced evaluation of the model's performance. Accuracy measures the overall correctness of predictions, considering true positives and true negatives. Our "Proposed" framework consistently outperforms [16] and [17]across all dataset sizes concerning F-measure. The higher F-measure values of our framework highlight its superior balance between precision and recall, affirming its effectiveness in achieving accurate positive predictions and comprehensive coverage of positive instances.

In terms of accuracy, the "Proposed" framework exhibits superior performance compared to the comparative algorithms. This implies that our framework attains a higher percentage of correct predictions overall, further affirming its improved performance. Our proposed framework's superior F-measure can be elucidated by its capacity to offer accurate positive predictions while maintaining comprehensive coverage of trustworthy cloud service providers. This equilibrium is influenced by the dynamic optimization capabilities of the Firefly Algorithm, which effectively balances precision and recall. The literature on optimization algorithms supports this balance, emphasizing its importance in solving complex problems. Accuracy, as a broader measure of the correctness of predictions, is achieved through the synergy of the Firefly Algorithm and Ant Colony Optimization. The high accuracy rates can be attributed to our framework's ability to optimize resource allocation while considering trust levels. The comprehensive approach ensures that not only trustworthy providers are selected but also that resource allocation is tailored to changing workloads, which can fluctuate over time.

These results are aligned with previous research emphasizing the effectiveness of hybrid frameworks incorporating optimization algorithms and privacy-preserving techniques for enhancing trust and resource allocation in cloud computing. The "Proposed" framework's superior F-measure and accuracy values reinforce its potential for real-world applications, especially in contexts where trust and privacy are of utmost importance.

The novelty of this work lies in its innovative combination of the Firefly Algorithm, Ant Colony Optimization (ACO), and privacy-preserving computation techniques within a unified framework for improving trust and privacy in cloud computing services. While each of these elements has been individually explored in previous research, their fusion within a comprehensive framework represents a novel approach to addressing trust, resource allocation, and privacy issues in cloud computing. Here's how the results are more relevant and novel in this context: (1) Integration of Advanced Algorithms: The proposed work integrates the Firefly Algorithm and Ant Colony Optimization. While these algorithms have been studied separately for optimization problems, combining them for trust generation and resource allocation in the context of cloud services is a novel approach. The results demonstrate the superiority of this integrated approach over existing methods. (2) Comprehensive Trust and Privacy Considerations: The framework not only focuses on optimizing resource allocation but also emphasizes trustworthiness and privacy. Prior research often addresses one aspect at a time, but this work provides a holistic solution by simultaneously improving trust and preserving data privacy. The results confirm that this comprehensive approach yields higher precision, recall, F-measure, and accuracy, making it more relevant for real-world applications where both trust and privacy are critical. (3) Advanced Privacy-Preserving Techniques: The proposed work

utilizes advanced privacy-preserving techniques such as differential privacy and homomorphic encryption, along with Secure Multi-Party Computation (SMPC) for collaborative computation. These techniques are crucial for maintaining data privacy in cloud environments and ensure that computations can be performed on sensitive data without exposing private information. The results underscore the effectiveness of these techniques in improving accuracy and trustworthiness. (4) Relevance to Current Cloud Computing Challenges: With the increasing importance of cloud computing in various domains, trust and privacy concerns have become paramount. The proposed framework addresses these contemporary challenges, making the results highly relevant to the current cloud computing landscape. The higher precision, recall, F-measure, and accuracy achieved by the proposed work are evidence of its ability to provide effective solutions to these challenges. (5) Comparative Analysis: The results are supported by a comparative analysis with state-of-the-art algorithms ([16] and [17]). This comparison demonstrates that the proposed framework outperforms existing approaches across various performance metrics. It highlights the novelty and relevance of this work in terms of achieving superior results in trust generation, resource allocation, and data privacy.

In summary, the novelty of this work lies in its holistic approach to address trust, resource allocation, and privacy concerns in cloud computing. The results presented in this study confirm that this innovative framework outperforms existing methods, making it a more relevant and novel solution for contemporary cloud computing challenges. These results indicate its potential for real-world applications where trust and privacy are paramount.

V. CONCLUSION AND FUTURE SCOPE

The evaluation of the proposed algorithm for trust generation, compared to Adil and Ahmad et al., demonstrates its superiority in terms of precision, recall, F-measure, and accuracy. The improved firefly algorithm utilized in the proposed approach plays a vital role in achieving these superior results. Privacy preservation is a critical aspect in the context of trust generation, and the use of an advanced firefly algorithm in the proposed work enhances privacy preservation capabilities. The higher precision achieved by the proposed algorithm indicates that it retrieves a larger proportion of relevant instances while minimizing false positives. This is crucial for privacy preservation as it reduces the risk of revealing sensitive information incorrectly. Additionally, the proposed algorithm exhibits significantly higher recall compared to Adil and Ahmad et al., suggesting its ability to capture a larger proportion of actual positive instances. This is essential for maintaining privacy and anonymity by minimizing false negatives, and ensuring that relevant instances are not overlooked or missed.

The higher F-measure of the proposed algorithm signifies a balanced trade-off between precision and recall, indicating its effectiveness in achieving accurate positive predictions and comprehensive coverage of positive instances. This balance is crucial for privacy preservation as it ensures a more accurate identification and classification of relevant instances while minimizing the risk of misclassification. Moreover, the superior accuracy of the proposed algorithm further reinforces its effectiveness in preserving privacy. The higher percentage of correct predictions overall indicates its ability to handle data more accurately and reliably, reducing the chances of privacy breaches and ensuring the integrity of sensitive information. In terms of scientific contribution, this work advances the field of privacy-preserving trust generation by introducing an improved firefly algorithm, which enhances the privacy preservation capabilities of the trust generation process. Our findings open the door to further research opportunities in the domain of privacy-preserving algorithms, trust management, and data privacy, paving the way for more robust and secure applications in various domains. Future research could explore additional enhancements to the proposed algorithm, investigate its applicability in different contexts, and explore novel methods for privacy preservation in trust management systems.

REFERENCES

[1] K. Munir and S. Palaniappan, "Secure Cloud Architecture," *Advanced Computing: An International Journal*, vol. 4, no. 1, pp. 9–22, Jan. 2013, doi: 10.5121/ACIJ.2013.4102.

[2] A. R. Arunarani, D. Manjula, and V. Sugumaran, "Task scheduling techniques in cloudcomputing: A literature survey," *Future Generation Computer Systems*, vol. 91, pp. 407–415, Feb. 2019, doi: 10.1016/J.FUTURE.2018.09.014.

[3] C. L. Philip Chen and C. Y. Zhang, "Data-intensive applications, challenges, techniquesand technologies: A survey on Big Data," *Information Sciences*, vol. 275, pp. 314–347,Aug. 2014, doi: 10.1016/J.INS.2014.01.015.

[4] I. Yaqoob *et al.*, "Big data: From beginning to future," *International Journal ofInformation Management*, vol. 36, no. 6, pp. 1231–1247, Dec. 2016, doi: 10.1016/J.IJINFOMGT.2016.07.009.

[5] A. Qadeer and M. J. Lee, "DDPG-Edge-Cloud: A Deep-Deterministic Policy Gradient based Multi-Resource Allocation in Edge-Cloud System," in *2022 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, pp. 339–344, 2022.

[6] L. S. Lee and W. D. Brink, "Trust in Cloud-Based Services: A Framework for Consumer Adoption of Software as a Service," *Journal of Information Systems*, vol. 34, no. 2, pp.65–85, Jun. 2020, doi: 10.2308/ISYS-52626.

[7] Q. Zhang, L. T. Yang, A. Castiglione, Z. Chen, and P. Li, "Secure weighted possibilistic c-means algorithm on cloud for clustering big data," *Information Sciences*, vol. 479, pp. 515–525, Apr. 2019, doi: 10.1016/J.INS.2018.02.013.

[8] B. C. Kara and C. Eyupoglu, "Anonymization Methods for Privacy-Preserving Data Publishing," pp. 145–159, 2023, doi: 10.1007/978-3-031-09753-9_12.

[9] G. Sun, L. Song, D. Liao, H. Yu, and V. Chang, "Towards privacy preservation for 'check-in' services in location-based social networks," *Information Sciences*, vol. 481, pp. 616–634, May 2019, doi: 10.1016/J.INS.2019.01.008.

[10] J. Wang, H. Li, F. Guo, W. Zhang, and Y. Cui, "D2D big data privacy-preserving framework based on (a, k)-anonymity model," *Mathematical Problems in Engineering*,vol. 2019, 2019.

[11] X. Zhang *et al.*, "Proximity-aware local-recoding anonymization with mapreduce for scalable big data

privacy preservation in cloud," *IEEE transactions on computers*, vol. 64, no. 8, pp. 2293–2307, 2014.

[12] J. Wang, H. Li, F. Guo, W. Zhang, and Y. Cui, "D2D big data privacy-preserving framework based on (a, k)-anonymity model," *Mathematical Problems in Engineering*,vol. 2019, 2019.

[13] K. Arava and S. Lingamgunta, "Adaptive k-Anonymity Approach for Privacy Preserving in Cloud," *Arabian Journal for Science and Engineering 2019*, vol. 45,no. 4, pp. 2425–2432, Jul. 2019, doi: 10.1007/S13369-019-03999-0.

[14] T. Kanwal *et al.*, "A robust privacy-preserving approach for electronic health records using multiple datasets with multiple sensitive attributes," *Computers \& Security*, vol. 105, p. 102224, 2021.

[15] R. Gangarde, A. Sharma, A. Pawar, R. Joshi, and S. Gonge, "Privacy Preservation in Online Social Networks Using Multiple-Graph-Properties-Based Clustering to Ensure k-Anonymity, l-Diversity, and t-Closeness," *Electronics*, vol. 10, no. 2877, pp. 1–21, 2021, doi: 10.3390/electronics.

[16] N. Ahmed, A. L. C. Barczak, M. A. Rashid, and T. Susnjak, "Runtime prediction of big data jobs: performance comparison of machine learning algorithms and analytical models," *Journal of Big Data*, vol. 9, no. 1, p. 67, 2022.

[17] M. Adil, S. Nabi, M. Aleem, V. G. Diaz, and J. C.-W. Lin, "CA-MLBS: content-awaremachine learning based load balancing scheduler in the cloud environment," *Expert Systems*, vol. 40, no. 4, 2022, doi: 0.1111/exsy.13150.

[18] D. Li, J. Wang, Q. Li, Y. Hu, and X. Li, "A privacy preservation framework for feedforward-designed convolutional neural networks," *Neural networks : the official journal of the International Neural Network Society*, vol. 155, pp. 14–27, Nov. 2022, doi: 10.1016/J.NEUNET.2022.08.005.

[19] M. Zivkovic, N. Bacanin, J. Arandjelovic, I. Strumberger, and K. Venkatachalam, "Firefly algorithm and deep neural network approach for intrusion detection," in *Applications of Artificial Intelligence and Machine Learning: Select Proceedings of ICAAAIML 2021*, Springer, pp. 1–12, 2022.

[20] D. Jovanovic, M. Antonijevic, M. Stankovic, M. Zivkovic, M. Tanaskovic, and N. Bacanin, "Tuning machine learning models using a group search firefly algorithm for credit card fraud detection," *Mathematics*, vol. 10, no. 13, p. 2272, 2022.

[21] M. Yang *et al.*, "A trusted de-swinging k-anonymity scheme for location privacy protection," *Journal of Cloud Computing*, vol. 11, no. 1, pp. 1–15, Dec. 2022, doi: 10.1186/S13677-021-00272-4/FIGURES/11.

[22] H. Godhrawala and R. Sridaran, "Improving Architectural Reusability for Resource Allocation Framework in Futuristic Cloud Computing Using Decision Tree Based Multi-objective Automated Approach," in *Advancements in Smart Computing and Information Security: First International Conference, ASCIS 2022, Rajkot, India, November 24--26, 2022, Revised Selected Papers, Part I*, pp. 397–415, 2023.

[23] M. Duraid Abdul-Jabbar and Y. Abdul alsahib saldeen Assist, "State-of-the-Art in Data Integrity and Privacy-Preserving in Cloud Computing," *Journal of Engineering*, vol. 29, no. 1, pp. 42–60, Jan. 2023, doi: 10.31026/J.ENG.2023.01.03.

[24] B. Su, J. Huang, K. Miao, Z. Wang, X. Zhang, and Y. Chen, "K-Anonymity Privacy Protection Algorithm for Multi-Dimensional Data against Skewness and Similarity Attacks," *Sensors 2023, Vol. 23, Page 1554*, vol. 23, no. 3, p. 1554, Jan. 2023, doi: 10.3390/S23031554.

[25] G. Dagadu Puri and D. Haritha, "Implementation of Big Data Privacy Preservation Technique for Electronic Health Records in Multivendor Environment," *IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 14, no. 2, p. 2023, Accessed: May 11, 2023. [Online]. Available: www.ijacsa.thesai.org

[26] H. Jiang, J. Pei, D. Yu, J. Yu, B. Gong, and X. Cheng, "Applications of Differential Privacy in Social Network Analysis: A Survey," *IEEE Transactions on Knowledge andData Engineering*, vol. 35, no. 1, pp. 108–127, 2023, doi: 10.1109/TKDE.2021.3073062.

[27] X. Hu, T. Zhu, X. Zhai, W. Zhou, and W. Zhao, "Privacy Data Propagation and Preservation in Social Media: a Real-world Case Study," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 4, pp. 4137–4150, 2021, doi: 10.1109/TKDE.2021.3137326.

[28] C. Marche, L. Atzori, V. Pilloni, and M. Nitti, "How to exploit the Social Internet of Things: Query Generation Model and Device Profiles' Dataset," *Computer Networks*, vol. 174, p. 107248, Jun. 2020, doi: 10.1016/J.COMNET.2020.107248.

[29] SIoT, "Social Internet of Things," 2022. http://www.social-iot.org/ (accessed Oct. 18, 2022).

[30] X.-S. Yang, "Firefly algorithm, stochastic test functions and design optimisation," *International journal of bio-inspired computation*, vol. 2, no. 2, pp. 78–84, 2010.

[31] N. Nayar, S. Gautam, P. Singh, and G. Mehta, "Ant Colony Optimization: A Review of Literature and Application in Feature Selection," Lecture Notes in Networks and Systems, vol. 173 LNNS, pp. 285–297, 2021, doi: 10.1007/978-981-33-4305-4_22/COVER.