2023

Survey of Multiple Clouds: Classification, Relationships and Privacy Concerns

Reem Al-Saidi
University of Windsor

Ziad. Kobti
University of Windsor

A Survey of Multiple Clouds: Classification, Relationships and Privacy Concerns

Reem Al-Saidi
School of Computer Science
University Of windsor
Windsor, Canada
Email:alsaidir@uwindsor.ca

Ziad Kobti
School of Computer Science
University Of windsor
Windsor, Canada
Email:kobti@uwindsor.ca

***Abstract*—When major Cloud Service Providers (CSPs) network with other CSPs, they show a predominant area over cloud computing architecture, each with different roles to serve user demands better. This creates multiple clouds computing environments, which overcome the limitations of cloud computing and bring a wide range of benefits (e.g., avoiding vendor lock-in problem). Numerous applications can use various multiple clouds types depending on their specifications and needs. Deploying multiple clouds under hybrid or public models has introduced various privacy concerns that affect users and their data in a specific application domain. To understand the nuances of these concerns, the present study conducted a survey to identify the various classifications of multiple clouds types and then extend the cloud entities' relationships to behave in different multiple clouds settings. The survey results outline users' privacy and data confidentiality concerns in multiple clouds types under public and hybrid deployment models.**

Keywords-multi-cloud; federated cloud; cross-federated cloud; hybrid federated cloud; inter-cloud; cloud interoperability; privacy; trust.

I. Introduction

Utilizing numerous clouds has emerged as an alternative way to improve cloud computing capacity for massive and real-time data [1] [2]. Collaboration and communication between clouds, known as "Cloud Interoperability" will improve data reliability and resource availability, resulting in high-quality services [3]. Moreover, allowing clouds to connect brings further benefits to the cloud users by avoiding vendor lock-in and getting access to widely distributed resources across different clouds with good performance and legislation-compliant services to the users [3]–[6]. Different applications which produce huge amounts of data realize the importance of multiple clouds to outsource their data and services for better processing and analysis. For example, in the Internet of Things (IoT) applications outsourcing the data to different clouds for further processing overcomes the devices' limited storage and processing capacities [2]. The devices are connected to the internet clouds to accommodate the massive amount of the produced data by each device; processing the data at the edge provides low latency, efficient computation capabilities, and storage capacities [2]. Despite multi-cloud's resource availability, data reliability and scalability [3]–[6], maintaining cloud interoperability while preserving users' privacy and data security is still a significant challenge [3]. Without the users' consent, their data can be stored in another CSPs with different access rules and data processing requirements [7]–[10]. Furthermore, it becomes difficult to guarantee that data is effectively protected through its entire life-cycle, including data creation, storage, processing, transfer, and deletion; different CSPs may have different security policies, methods, and procedures for data processing and storage [7]. It is also more challenging to guarantee the consistency of security policies across all CSPs during data transfer and access, and protect the data against potential threats [16]–[18]. Moreover, identifying the access roles and sharing privileges among different CSPs while maintaining user-sensitive attribute without performance degradation is another critical concern while deploying multiple clouds [22].

Different application domains benefit from multiple clouds deployments [2] [19] [20] [22]. In the health era, various health institutions can share their data and collaborate with other researchers and healthcare professionals, enabling real-time collaboration and improving personal health and treatments [22].

While multi-cloud facilitates seamless data exchange and sharing across different health institutions, it also raises privacy and security concerns concerning data access and sharing processes [58]–[61] [63], [64]. Unauthorized and unrestricted access could expose patient information, compromising privacy and confidentiality. Moreover, the unrestricted data sharing beyond the intended purpose increases privacy risks and the potential for data misuse. Considering the privacy and security issues across various cloud deployment models through different applications reduces the data disclosure risks and highlight the possibilities of applications vulnerabilities.

Without question, user privacy and data security are of the highest importance in the digital age and have attracted much more attention with the adoption of multiple clouds computing. The success of such adoption towards building trustworthy multiple clouds environments is primarily driven by cloud user privacy and data security [9] [10].

There is no generalization for specific security and privacy-preserving approaches in the multiple clouds. It is mainly based on a specific context and the entities involved under a specific multiple clouds type.

 ISBN: 978-1-68558-044-5

The main contributions of this survey are the following:

- Show the classification of multiple clouds types from the state-of-the-art work.
- Investigate the challenges for public and hybrid deployment models in multiple clouds types.
- Extend the single cloud entity's relationships to behave in different types of multiple clouds environment.
- Identify the privacy concerns in the multi-cloud, federated, cross-federated, and inter-cloud under public and hybrid deployment models at some application domains.

The rest of this survey is organized as follows: In Section II, we introduce different types of multiple clouds and their corresponding classification. In Section III, we highlight different difficulties and challenges associated with the various multiple clouds deployment models. In Section IV, we extend the cloud entities relationships to behave under different kinds of multiple clouds. In Section V, we explain the privacy issues in different multiple clouds types under hybrid deployment model. Where appropriate, we reflect these privacy concerns on some applications. Moreover, we highlight the main challenges of different cloud types under specific deployment models. In the end, in Section VI, we summarize the survey work and show the future directions.

II. Multiple clouds classification

Multiple clouds mean the connection of more than one cloud. It is similar somehow to the set of an inter-connected cloud of clouds. In [4], they introduced the inter-connected global clouds of clouds, it is called the "Inter-Cloud", in which clouds interact and share the resources and the underlying infrastructure to meet the user's on-demand requests. Inter-cloud dynamically allows the management of resources and distributes the loads among different clouds for better resource utilization and service performance. Most researchers consider multiple clouds the same as inter-cloud [1] [11] [12]. Both are classified into multi-cloud and federated cloud based on how clients interact with the clouds.

Inter-cloud is defined as a "maximal set of inter-connected clouds so that no other organization exists outside the inter-cloud domain" [12]. However, some researchers consider inter-cloud as a federated cloud [13] while others [12] claim that the federated cloud is a type of inter-cloud. In [13], they stated the main differences between federated and inter-cloud; the federated cloud is a pre-requisite to the inter-cloud. In a federated cloud, all federated members would have a common perceptive of the applications deployment process [29] [30] while the inter-cloud is based on standards and open interfaces [13]. Federated cloud promises to deploy in different fields, including the academic domain, by building the community cloud with grid computing [19] [20] [28]. Others [16] consider federated cloud as a multi-cloud with a hybrid deployment model.

Inter-cloud is classified into multi and federated clouds [11] [12]. Multi-cloud defines in [15] as "an evolution of cloud computing where different services like Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) are provided based on the organization demands from various cloud service providers".

Multi-cloud enterprises can get services from more than one CSP. It highlights two subcategories: the hybrid and rain cloud [16]. In a rain cloud, each cloud member completes a Service Level Agreement (SLA) with other members enabling different members to work together when data get too large for any of them to handle [17]. SLA works only in a single or private organization, and it is not reliable under public cloud systems [17] [45]. Based on the resources and service provisioning by the broker, multi-cloud is classified into two implementation categories: services and libraries [18]. The federation term refers to the organizational structure where multiple enterprises have set up collaborative agreements known as "Federated Level Agreements (FLA)" [19].

The federation facilitates the adoption of cloud computing within different companies; the private cloud is built internally within the enterprises' scope and connected when necessary to the public cloud for on-demand resource leasing [14] [19] [20]. The federation should be capable of allowing location-free virtual applications deployment across federated sites. These applications can migrate from one site to another partially or completely [19]–[21]. The objective of the federation is to allow collaboration and resource sharing among different cloud providers. It is more appropriate to deploy the federated cloud when a few businesses are willing to cooperate and share their resources to serve the cloud user better [19]–[21].

Signing FLA is simpler when there are a few organizations, it gets challenging when there are several. The user access to the CSP is transparent; which means that users benefit from the federated cloud without being aware of which cloud provider supports the service [21]–[23]. Federation construction among different service providers has many benefits (e.g., increasing the economy of scale, efficient use of the resources and assets, and expansion of providers capabilities) [23]. Maintaining security, privacy, and independence between the federation members is necessary for trustworthy cloud federation construction. There are two types of federated cloud: horizontal federation and cross-cloud federation [1] [24].

The horizontal federation takes place on one level of the cloud stack, e.g., the application stack. Customers may profit from lower costs and better performance, while providers may offer more sophisticated services [1] [23]–[26]. The disadvantage of the horizontal federation is the lack of services scalability and diversity, it can not dynamically meet the changing customers' needs in the application.

Most CSPs that offer comparable services are horizontally federated; the members of the federation offer slightly different services. Thus, limiting the ability of the federated members to scale once user demands for new services increase. Furthermore, while CSPs compete with one another to increase their benefits and reputation, they are reluctant to pool resources or work together in specific contexts, thus limiting the diversity of services offered [23]–[26].

From the developer's point of view, the infrastructure management of federated cloud is easy to develop and maintain

 ISBN: 978-1-68558-044-5

through the different federation members via a standard Application Programming Interface (API) [11].

The federation achieves a traffic load balancing among the members to accommodate unusual spikes in resource demands [23] [24]. Moreover, building a federation is less costly than each organization expanding its infrastructure [1] [23] [24]. Implementing a federated cloud overcomes the vendor lock-in problem associated with a single cloud and provider integration concerns [24]. However, federation still suffers from the contention problem where in [27]–[30] addressed the issue and suggested a solution accordingly.

There are many challenges with the federation construction (e.g., performance and disaster recovery through co-location and geographic distribution, expressing the FLA requires translating the abstract requirements to understandable properties for effective organization implementation, and supporting the vertical expansion of the service layer [24]).

In the cross-cloud federation [6], two or more unfamiliar CSPs agree to collaborate during run time. It provides dynamic and diverse benefits to CSPs for expanding their service at run time to better serve the users changing demands. Still, the main challenge in the cross-cloud federation is building the chain of trust from the cloud user to the home cloud, followed by a series of foreign cloud-transitive trust [1]. Another challenge is finding a standardized interface for resource access among cloud domains each with different architectures, policies, and implementations [6].

In [1], they show the several phases of the cross-cloud federation, starting from the discovery of another CSP, called "Foreign Cloud," that wishes to share its federated resources. The home CSP triggers the need for resource leasing as it can not serve the user's requests. The foreign CSP has the minimum user specifications, it will lease its additional federated resource, and be part of the federation construction. The foreign CSP can either have the same requested service forming the intralayer or can pass the request through its stack and delegate the process to the middleware to install the required service forming the interlayer [26].

A Cross-Cloud Federation Manager (CCFM) is the trusted party that makes the negotiations with the foreign cloud, starting from the discovery and resource matching ending with the resource access. CCFM bridges the gap between different service providers through various stages [1] [6].

In conclusion, several perspectives exist on classifying multiple clouds; some consider federated clouds as inter-cloud [13]. Others disagree and claim that federated cloud is a type of inter-cloud [12]. The following classification outlines our categorization of multiple clouds; the inter-cloud is the main category of multiple clouds, classified into multi-cloud and federated clouds. The federated cloud has two main subtypes: horizontal federation and cross-cloud federation.

From our perspective, Figure 1 summarizes the classification of different cloud types.

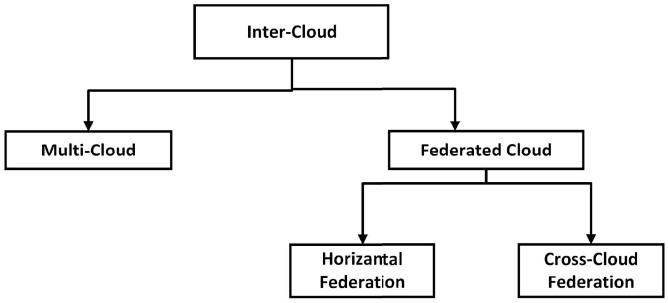

Figure 1: Multiple clouds classification.

III. Difficulties with multiple clouds deployment models

Multiple clouds consist of different elements that can be varied based on specific cloud types and application domains [30]. Moreover, there are different deployment models, including private cloud, public cloud, hybrid cloud, and community cloud [31]. Each deployment model implemented among different types of multiple clouds introduces a wide variety of challenges [32].

Private cloud [21] [31] [32] is a specific computing infrastructure owned and controlled by an organization (enterprise) to serve a group of users in a specific application domain. It can be classified in two main categories:

- Cloud portfolio, in which more than private cloud belongs to the same organization share the same private cloud infrastructure. They didn't compete with each other as they belong to the same organization domain. They can easily initiate cooperation requests with each other and increase the organization revenues [12].
- Independent, a separate cloud each with its own infrastructure and resources and not forming a part of cloud portfolio [21] [32] .

Generally, the private cloud has several challenges and issues including vendor lock-in, trust, security and privacy, cost, scalability and availability [21] [32]. Public cloud [33]–[35] in which prominent vendors and well-known service providers support a wide range of competing services in the marketplace. The services are available to a wide range of interested users upon subscription. The public cloud deployment model supports a multi-tenant feature of cloud computing where different users can share the same pool of storage infrastructure [33]–[36] [46].

Still, deploying the public cloud faces different challenges and concerns [31] [32] [34]–[36], mainly the trust issue becomes the most evident one under the uncertainty and loss of control in the multiple clouds environment. Building trust in the public cloud towards their users will assure them about their data confidentiality and cloud provider commitment and ethical behavior. Implementing a secure infrastructure while keeping the privacy of user attribute and data with a high level of assurance is the first step towards building a trustworthy multiple clouds environment. However, the communication

 ISBN: 978-1-68558-044-5

between private and public clouds forms a hybrid deployment model known as "Cloud bursting" in which a private cloud can extend its resource by initiating a request to an external provider as it can't serve its user demands [37]. Even deploying the hybrid model shows promise of enabling cloud interoperability and scalable services provisioning, it still faces many challenges and issues [37]–[40]. The main challenges and concerns in hybrid deployment model are:

1. Trust [38] [39] : trusted entities like a broker or middleware facilitate communication among cloud entities and monitor resource provisioning and access processes between private and public clouds. Cloud users should trust the public cloud provider as they will lose control over their outsource data and services running over the public cloud. A high degree of trust is required so that more users can join a public provider and benefit from its services and applications.
2. Security and privacy [40]: different security regulations and privacy compliance control user data and cloud provider behavior. Due to the lack of user control and the high level of users' uncertainty about the public cloud's commitment. Different privacy and security techniques should be implemented during all data life cycles highlighting different contexts and scenarios.

On the community cloud deployment, resources are owned and controlled by different cloud providers in the community [41]. It has a security and privacy concerns as same as the other deployment models [41].

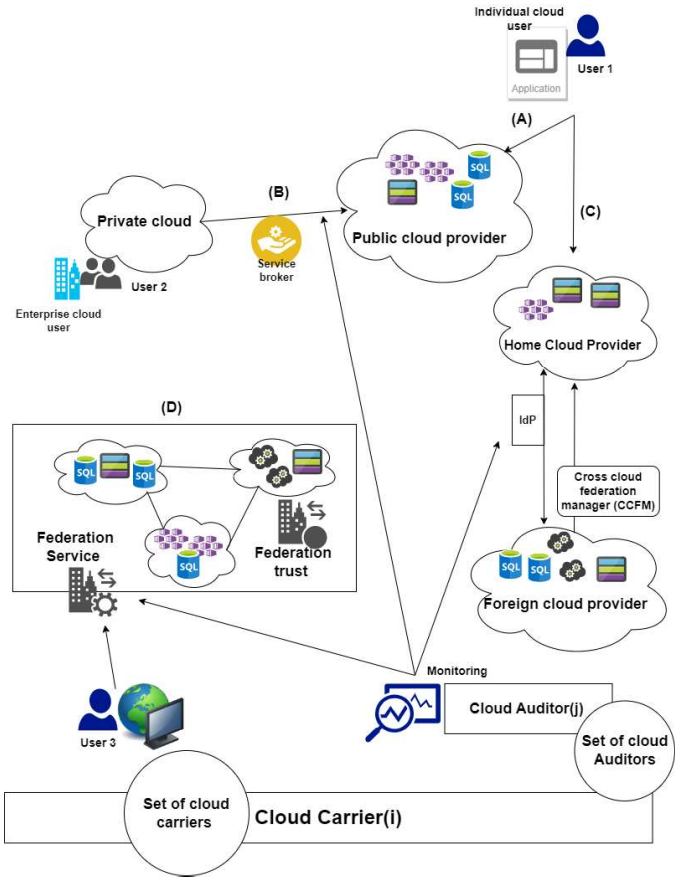

Figure 2: Multiple clouds types entities relationship.

IV. Entities' relationships on multiple clouds

NIST [42] defined the cloud's five main components: cloud users/consumers, providers, carriers, auditors, and brokers. Each of these entities has different tasks based on a specified setting. We will consider the same entities in the context of multiple clouds and extend their interactions and relationships to behave in a distributed manner. Multiple clouds consist mainly of cloud user(s), cloud provider(s), cloud auditor(s), cloud trusted party as broker(s) or identity providers (IdPs), and cloud carrier(s).

The entities have a context relationship determined by user activities and the type of multiple clouds in use. They have the same definition provided by NIST [42] with some extensions to accommodate the distributed nature of multiple clouds. The elements form the multiple clouds, and their definitions [42] are listed below:

1) Cloud user/consumer(s) are an enterprise, or individuals with internet access looking for better services to meet their demands.
2) Cloud providers/ data center(s) are vendors that offer different types of services (platform, infrastructure, storage, software, artificial intelligence functionalities) on different domains. It supports cloud users with different service and resource leasing based on a pre-defined signed agreements.
3) Cloud-trusted entities facilitate a reliable service delivery between users and providers or among providers themselves. The trusted entities vary based on the type of cloud, e.g., brokers used in the federated, inter-cloud, and cross-cloud federation with an intermediate role. The trusted entities can assist the customer in selecting the most suitable service, manage the dimensionality, heterogeneity, and user uncertainties towards their data and the CSPs [43].

   Brokers in inter or meta cloud can handle the discovery of suitable resources and subsequent data life cycle management [11]. In the context of a cross-cloud federation, the trusted party CCFM is used in the discovery, resource matching, and authentication between home and foreign clouds when the first is saturated in its resources [25]. IdPs act as trusted entities in the cross-cloud federation to establish trust and secure communication between home and foreign clouds for resource access and sharing [1] [25].
4) Cloud auditor(s) perform an assessment of services, performance and security to comply to the regulations and the pre-defined agreements between different entities in the cloud.
5) Cloud carrier(s) support the connectivity and transformation of the cloud services in the underlying network infrastructure across different clouds.

The last two entities are also mentioned in [44]. Different

types of relations control the communication among multiple clouds entities. We use a formula notation to analyze the interactions and relations between various cloud entities under different types of multiple clouds, which facilitates describing the inputs, outputs, and transformations that take place during a specific interaction. Moreover, the formula notation will provide a structured model approach to describe sophisticated scenarios in multiple clouds [42] [44]. The relation depends on a specific application context and the corresponding multiple clouds type deployed. Figure 2: (A, B, C, D) shows the different entities' relationships under different multiple clouds type. A and B describe entities relationship in the multi-cloud with a hybrid deployment model. C illustrates the cross-cloud federation entities relationship, and finally, D represents the federation entities interaction relationship.

The following are the main entities and notations that used in explaining the four main relations depicted in Figure 2.

Main entities: cloud user(s), cloud provider(s), cloud broker(s), middle ware, cloud auditor(s) and cloud carrier(s).

Notation: cloud user i (U_i), cloud provider i (CP_i), relation ij R(ij): $U(\mathrm{i}) \implies CP(\mathrm{j})$ a relation from user i to cloud provider j, where $i \in \{1, 2, 3, \ldots, n\}$, $j \in \{1, 2, 3, \ldots, m\}$ and $n, m \in (N)$. N is the set of natural numbers.
It does not necessarily for n and m to be equal due to the cloud multi-tenancy feature [46].

A. Multi-cloud setting: individual user access a public cloud service provider.

Cloud users contact different cloud providers for better services provisioning and extra resources access. They can request various services from various CSPs to satisfy users' demands and needs. **Equation** (1) represents Ri between U_i and CP_j

$$U_i \implies CP_j \tag{1}$$

, where $U(\mathrm{i})$ represent an individual user. Moreover, the SLA controls the communication and the amount of leased resources between cloud users and CSPs. Also, a private cloud that needs extra resources to run its application and better meet its clients' needs can initiate a request to the public cloud. Figure 2: (A) demonstrates user 1 accessing a resource from a public cloud provider using an electronic device.

Trusted entities can be involved to monitor communication as a broker or middleware [45]. Cloud carriers and auditors are applied to assess the service delivery, the privacy and security compliance while supporting the connectivity for the underlying network infrastructure [42]. These have same rules as the single cloud, they can be replicated through the multiple clouds architecture design to behave in a distributed environment and avoid single point of failure. Noted that a cloud provider can serve different users at the same time, meeting a multi-tenancy feature of the cloud [46].

B. Multi-cloud setting: enterprise with its own private cloud access a public cloud service provider.

Users can be an individual working in an organization that holds its own private cloud. However, at specific point of time the private cloud could ask for extra resources or services from a well known cloud vendor, public cloud. This forming a hybrid cloud known as "Cloud Bursting" [37].

Equation (2) represents Rij between CP_i and CP_j.

$$CP_i \implies CP_j \tag{2}$$

However, a cloud provider can serve different users requests at the same time in a sharing and distributed environment maintaining the multi-tenancy feature. Figure 2: (B) shows user 2,the enterprise, running its own private cloud access resources from public cloud.

C. Cross cloud federation.

A cloud provider that lacks resources at specific point of time, home cloud, can dynamically request and get access to the resources from foreign cloud. IdP acts as a trusted point between home and foreign clouds for a secure communication and resource access. A CCFM is another involved trusted party for resource discovery, matching and authentication between the two clouds [1]. The contract for the communication obligation and rules are established dynamically and monitored by the cloud auditor or another motioning technique based on the cloud setting. Cloud auditors assess the service delivery performance and the compliance to the signed agreements. The cloud carrier supports the connectivity for the underlying network infrastructure. Figure 2: (C) shows the entities relationship in a cross-cloud federation where user 1 access can not be satisfied by his/her home cloud. Thus, initiated a dynamic request to foreign cloud that might serve user request. **Equation** (3) represents a dynamic relation denoted by RijD between CP_i (home cloud) and CP_j (foreign cloud) [Cross-cloud federation].

$$CP_i(Home) \implies CP_j(foreign) \quad \text{Dynamic} \tag{3}$$

D. Cloud federation.

In a federated cloud, when a cloud provider has a shortage on it resources and limitation in it underlying infrastructure to run an application, it can statically sign an agreement with another provider to overcome the resource shortage and limitation on its underlying infrastructure [19]–[21], forming a federation.

A cloud broker facilitates collaboration and monitoring across different federation members [43] [45]. Cloud auditors assess the service delivery performance and the compliance to the signed agreements. The cloud carrier supports the connectivity for the underlying network infrastructure.
Figure 2: (D) shows the entities relationship in a cloud federation where user 3 can transparently access different

services offered by federated members.

Users' access can be transparently served by any federation members that statically pre-signed an agreement regulating their communication and service provisioning. **Equation** (4) represents a static relation denoted by RijSt between CP_i and CP_j.

$$CP_i \implies CP_j \qquad \text{Static} \qquad (4)$$

V. Privacy concerns in different types of multiple clouds

Privacy concerns become the most critical challenge in multi-cloud while maintaining cloud interoperability. In this section, we will explore the privacy concerns raised by various types of multi-cloud.

A. Multi-cloud with hybrid deployment model

Many enterprises with private cloud infrastructure access different services offered from various public cloud providers. The enterprises get many benefits; avoid vendor lock-in with better and cost-effective resource provisioning to their users, greater flexibility, increased efficiency, and more scalability [30] [38]. We assume no trusted parties are deployed with this model as it is difficult to establish and maintain trust and its corresponding relationship in the open, distributed and changing multiple clouds environment. Other privacy challenges include setting the regulations, pre-defined agreements, policies construction, cloud provider commitments, risk management, and ethical behavior towards the involved entities. We focus on user privacy as they are the main actors in the multi-cloud setting. However, the multi-cloud with hybrid deployment model, from our point of view, raises two primary users' privacy concerns:

1) Users' authentication and access privacy.

Users' have to authenticate themselves to access their outsourced data and different services from the public cloud providers. Users can be an individual with their own electronic device, denoted in Section IV by Ri relation, or users can be enterprises with their own private cloud where access are from private cloud to hybrid cloud, denoted in Section IV by Rij.

However, the authentication process reveals user identities, locations, habits and attributes to the cloud provider. There is no guarantee for cloud providers' ethical behavior towards cloud users and their corresponding attributes. Attackers can also monitor user behaviors and access patterns to derive sensitive information about the users and their valuable assets.

In the Cloud-based Vehicular Ad-Hoc Networks (VANET), each sensor node gathers real-time vehicle information and monitors its traffic route—all of this information is outsourced to the cloud to provide different cloud services [75]. Moreover, the sensor nodes can communicate with each other. The communication messages are aggregated to broadcast to a specific group of users in the VANET framework [76]. Through the various forms of communication, each vehicle must independently authenticate itself to sensor nodes to access a particular service. A typical vehicular communication message contains the vehicle's location, direction, and speed. The malicious entity might extract crucial driver information from those communications and use it to impersonate other vehicles identity and deliver false messages that could cause collisions and, at worst, the loss of human lives. Moreover, an intelligent transportation system needs access to the vehicle's location to generate real-time traffic reports and suggest various Points Of Interest (POI) [75] [76]. For such a purpose, driver semantic data for the visited places and current locations had to be extracted. These sensitive details reveal the user's lifestyle and routine. Keeping the privacy of the vehicle or sensor node's identity and information during the communication while enabling each node to authenticate itself privately without disclosing its associated information is cruical in VANET [77].

To sum up, the main privacy concerns in the multi-cloud setting are user authentication and access privacy, which entail identity, attributes, access patterns, and location privacy. These privacy issues are reflected during the vehicle authentication and communication procedure in the cloud-based VANET. Additionally, creating a traffic report in VANET necessitates access to the vehicle's location, which can reveal user habits.

2) Users' data security.

Users' lose control over their outsourced data. If it is transfer in plain format, it will be posed to a different type of disclosure and attacks. Also, it can be easily modified, which affects its integrity and completeness. Encrypted data before outsourcing to maintain its confidentiality adds extra load to the enterprise side, which usually has limited performance capacities and storage space. Moreover, the encryption of the data requires pre-communication between private and public clouds to set private and public keys in the case of public key techniques. More advanced cryptographic techniques (e.g, full homomorphic encryption [57]) are used to encrypt the data to permit operations over the outsource encrypted data.

However, those advanced techniques add extra complexity to the infrastructure which could affect the application usability and performance. Moreover, users' data transferred through other cloud providers could face different policies and access procedures. Another privacy concern is the operation performed by authorized entities over the outsourced data.

Querying the data stored in distributed database cloud storage poses various privacy concerns. We demonstrate query privacy in the multi-cloud genomic application. Many authorized researchers and health organizations query the outsourced encrypted genome data stored in different cloud databases. The query statement searches a cloud database first to meet specific criteria stated in the conditional part of the query and get the result back.

The query details include contents (e.g., conditional part and indices position), outcome, target, and user access pattern. In the context of genomic data, knowing any query contents by unauthorized or malicious entities will reveal sensitive information (e.g., in the genomic sequence, the location of a specific DNA pattern will indicate the type of patient disease). The specific pattern and location detected in the patient determine the classification of the disease in some

 ISBN: 978-1-68558-044-5

forms of diabetes, such as Maturity-Onset Diabetes of the Young (MODY) [72]. In [73] [74], they succeeded in securely querying private in genomic datasets to discover which specific genomic alterations are associated with a disease, thus increasing the availability of these valuable datasets. Ensuring the privacy of the query so that the cloud provider will not be able to deduce any information from the query except what is allowed to do, and the researcher will not know any other information on the genomic database. Finally, choosing the most appropriate privacy-preserving techniques that could be applied efficiently, securely, and scalably when inquiring about genomic data is crucial in the genomic domain.

To summarize, user data security entails its confidentiality, integrity, availability, and access rights management, which are other critical privacy concerns in the multi-cloud hybrid deployment model. Moreover, different privacy concerns can be determined based on a specific application context, data sensitivity, application requirements, and entities involved in a particular cloud type.

B. Federated cloud.

1) Horizontal federation architecture.

Cloud providers set pre-defined rules and policies to integrate and establish a federation [1] [19]–[22]. The established regulations, policies, and trust govern the communication between federation members. Users get a wide variety of services from the federation transparently, denoted in Section IV by RijSt. However, this type of federation is usually static; if the user wants service outbound to the federation capacities, the user request is denied [1] [19]–[22]. There is also a high possibility of malicious attacks during the members' communication, thus affecting the confidentiality of data and threatening user privacy [47]. Also, there is no guarantee that a subset of federation members collude to extract user-sensitive information.

Moreover, there are many security challenges in constructing a federated cloud [48], which are the longer chain of trust, limited audibility, risk of malicious service components, and liability and legal issues. The users in federated cloud and inter-cloud will face the same privacy concern as those on the multi-cloud hybrid deployment model. Integration of end-to-end security and privacy implementation in the federated cloud is the undergoing research area which is challenging to balance the efficiency and security in the federation implementation [47].

2) Cross-federated cloud and inter-cloud.

When a user wants a service not supported by the cloud provider in which customer is subscribed to and trusted, the cloud provider can collaborate on-fly with another cloud provider to satisfy the user's demands. The corresponding relation denoted in Section IV by RijD. The CCFM is the trusted party that starts the resource discovery process till finding the appropriate cloud provider that best matches the request. Ending with the authentication between the home and foreign cloud providers to facilitate the access and resource provisioning processes [1].

The dynamic discovery put the involved entities at high risk in the open and untrusted multiple clouds environment. As there is no pre-defined trust in the dynamic discovery between the cloud providers, maintaining the dynamic trust, in that case, is becoming challenging. Different doubts surrounded trust itself: What is trust? Is it a vulnerability to the system or not? What is the type of trust that could establish? What are the trust requirements and specifications in a dynamic context? What are the relationships between trust, risk, and assurance levels? Is trust enough to guarantee user privacy? What metrics are required to implement a privacy preservation approach in the inter-cloud and cross-federated cloud?

Moreover, identifying the risks will help mitigate undesirable circumstances that threaten user privacy. However, the risk will still depend on a specific context and what is considered valued and require a higher protection mechanism during the dynamic discovery, resource provisioning and access process. Identifying the relationships between trust and risk facilitates dynamic discovery decisions to federate or not [49] [50]. Cross-cloud federation shows its applicability in a wide range of domains starting from research and academia, engineering and construction, financial and industry, real-time data processing, and online gaming [1].

Inter-cloud facilitates the dynamic discovery of the resources in a wider scale domain. Within the federated identity management, user access different federated services and resources. Trust is an essential factor within the federated members to transparently satisfy the user better demands (e.g., a proxy certificate is used for trust implementation in the grid computing [51]).

Single sign-on (SSO) application under inter-cloud enables users to authenticate only once and get access to different web services located at other clouds without the need to be re-authenticated again. Different standard protocols were established in the SSO [52]. The two most popular are Security Assertion Markup Language (SAML 2.0) [53], and OpenID connect [54], each of them with its specifications and format [53] [54]. However, each generates an authentication/access token to delegate the authentication on behalf of the user. The authentication delegation allows access to specific attributes identified in the access token [55]. These protocols should prevent any impersonation and other malicious activities performed by the IdP (e.g., monitoring user access and linking user identities to different activities offered by service providers). Still, securing these protocols against attacks is challenging in web cloud domain. Many attacks are reported [56].

C. The hybrid deployment model under a federated cloud.

Integrating federated cloud with hybrid deployment model known as "Hybrid Federated Cloud Computing," which allows interoperability across different federations. The main objective of this type is to provide an environment with seem-

 ISBN: 978-1-68558-044-5

TABLE I: PRIVACY CONCERNS IN MULTIPLE CLOUDS TYPES.

Cloud type	Deployment model			Privacy concerns	Application
	Public	*Private*	*Hybrid*		
Multi-cloud			✓	• Identity privacy. • Location privacy. • Access pattern privacy. • Query privacy. • Data and access privacy.	• VANET. • Genomic domain.
Federated cloud			✓	• Risk of dynamic discovery. • Authentication privacy. • Access privacy.	Bio-informatic with SSO.
Horizontal federation	✓	✓	✓	• Trust between federation members: – No collude federated members. – longer chain of trust. • Identity privacy. • Risk of malicious service components. • Liability and legal issues. • Limited audibility.	Small organizations.
Cross-federated and inter-cloud			✓	• Identity privacy. • Attribute privacy. • Token access privacy. • Access and authorization privacy.	SSO (SAML 2.0, OIDC protocols)

ingly limitless computational resources, processing power, and storage space that can effectively meet user demands [52] [58]–[61]. In the bio-informatics domain, a bioNimbus [60] [61] is a federated cloud platform in which different independent, heterogenous, private/public/hybrid clouds are collaborated to support other bio-informatics applications. It maintains the internal configuration and privacy policies for each federation member.

BioNimbus supports on-demand resource provisioning in an efficient, flexible, fault tolerance, and scalable way under the hybrid horizontal federation deployment model [60]–[63]. It integrates different bio-informatic workflows for identifying differentially expressed genes in cancer tissue.

Various bio-informatics centers can benefit from the federation collaboration to access other data and have extra storage in a distributed, transparent, and fault tolerance way [62] [64]. The security, including authentication, authorization, and confidentiality, can be implemented in the hybrid federated cloud without adding extra dependency among the federation members through the standard SSO protocols OpenID and OAuth [64]. The user authenticates through their federation provider and gets access to other federation members. The access control list governs the access process based on the federation pre-signed federation agreement.

In [63], they suggest using the attribute-based access control for the bioNimbus operating under a federated cloud, which effectively guarantees that eligible users can only access resources without impacting the authorization response back time. However, when a federation requests additional resources from other public clouds or federations, privacy issues related to authentication and access should be addressed. These issues also include the risk of dynamic discovery and creating a new connection with an unknown federated cloud or cloud provider. Different projects [61] [63] [65]–[71] were implemented for bio-informatics applications under a federation cloud environment. Table I summarizes the privacy concerns within different multiple clouds types concerning various applications.

VI. Conclusion

The main goal of multiple clouds is to maintain cloud interoperability, allowing different clouds to communicate and interact to provide cloud users with a wide variety of resources and high-quality services. Moreover, multiple clouds get around a single cloud architecture limitation by allowing users to access various resources without being stuck to a specific cloud provider. There are different types of multiple clouds: cross-cloud, rain cloud, horizontal federation cloud, and federated cloud. Various applications deploy the cloud type that matches their specifications under public or hybrid deployment models.

Privacy is still of utmost importance in the digital world and has become vital for adopting different kinds of multiple clouds under a specific application domain. The success of multiple clouds adoption and a trustworthy environment is primarily driven by cloud security and preserving cloud users' privacy. The results of the present study's survey provide classifications of multiple clouds types and outline the most common multiple clouds taxonomy. The challenges for public and hybrid deployment models were investigated under different kinds of multiple clouds. For example, the most common concerns under the hybrid deployment model were privacy, security, and trust. However, the relationships that connect single cloud entities no longer suit the multiple clouds architecture; thus, for the purposes of the present study, the relationships were extended from a single cloud to behave under different kinds of multiple clouds in a distributed manner. As privacy is a key consideration when deploying multiple clouds, the study introduced different privacy concerns in various applications

 ISBN: 978-1-68558-044-5

that deploy a specific type of multiple clouds.

For example, the bio-informatic domain deploys a hybrid federated cloud, which raises authentication and access privacy concerns. Also, an SSO web application that deploys a cross-federated cloud will pose token access privacy, identity, and attributes privacy. The privacy concerns outlined in the study underscore the need to examine more applications that use multiple clouds and show the current solutions for handling these privacy issues. Moreover, a supplementary survey should explore the potential of developing new techniques for privacy preservation in multiple clouds.

Acknowledgments: We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC [funding reference number 03181]). We also acknowledge the input from Dr. Mahdi Daghmehchi Firoozjaei, School of Computer Science, University of Windsor.

REFERENCES

[1] U. Ahmed, I. Raza, and S. A. Hussain, "Trust evaluation in cross-cloud federation: Survey and requirement analysis," ACM Computing Surveys, vol. 52, no. 1. Association for Computing Machinery, Feb. 01, 2019. doi: 10.1145/3292499.

[2] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick, and D. S. Nikolopoulos, "Challenges and Opportunities in Edge Computing," in Proceedings - 2016 IEEE International Conference on Smart Cloud, SmartCloud 2016, Dec. 2016, pp. 20–26. doi: 10.1109/SmartCloud.2016.18.

[3] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, "Blueprint for the intercloud - Protocols and formats for cloud computing interoperability," in Proceedings of the 2009 4th International Conference on Internet and Web Applications and Services, ICIW 2009, 2009, pp. 328–336. doi: 10.1109/ICIW.2009.55.

[4] K. Keahey, M. Tsugawa, A. Matsunaga, and J. Fortes, "Sky computing," IEEE Internet Comput, vol. 13, no. 5, pp. 43–51, 2009, doi: 10.1109/MIC.2009.94.

[5] S. Shetty, A. P. Manu, V. Kumar, and C. Antony, "Need of Multi-Cloud Environment and Related Issues: A Survey," Journal of Xian University of Architecture & Technology, vol. 12, pp. 78-87, 2020.

[6] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "How to enhance cloud architectures to enable cross-federation," in Proceedings - 2010 IEEE 3rd International Conference on Cloud Computing, CLOUD 2010, 2010, pp. 337–345. doi: 10.1109/CLOUD.2010.46.

[7] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1. pp. 1–11, Jan. 2011. doi: 10.1016/j.jnca.2010.07.006.

[8] "Computer Communications and Networks." [Online]. Available: http://www.springer.com/series/4198. Accessed: March 2, 2023.

[9] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, "Cloud computing security: From single to multi-clouds," in Proceedings of the Annual Hawaii International Conference on System Sciences, 2012, pp. 5490–5499. doi: 10.1109/HICSS.2012.153.

[10] N. Thillaiarasu and S. Chenthurpandian, "Enforcing security and privacy over multi-cloud framework using assessment techniques," in Proceedings of the 10th International Conference on Intelligent Systems and Control, ISCO 2016, Oct. 2016. pp. 1-6, doi: 10.1109/ISCO.2016.7727001.

[11] Y. Elkhatib, "Mapping cross-cloud systems: Challenges and opportunities," in 8th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 16), pp. 1-5, 2016.

[12] N. Grozev and R. Buyya, "Inter-Cloud architectures and application brokering: Taxonomy and survey," Softw Pract Exp, vol. 44, no. 3, pp. 369–390, Mar. 2014, doi: 10.1002/spe.2168.

[13] A. N. Toosi, R. N. Calheiros, and R. Buyya, "Interconnected cloud computing environments: Challenges, taxonomy, and survey," ACM Computing Surveys (CSUR), vol. 47, no. 1, pp. 1-47, 2014.

[14] M. R. M. Assis and L. F. Bittencourt, "A survey on cloud federation architectures: Identifying functional and non-functional properties," Journal of Network and Computer Applications, vol. 72. Academic Press, pp. 51–71, Sep. 01, 2016. doi: 10.1016/j.jnca.2016.06.014.

[15] D. Gurusamy and T. K. Elemo, "Direct-cloud, multi-cloud, and connected-cloud – terminologies make a move in cloud computing," International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 2, pp. 386–393, Jul. 2019, doi: 10.35940/ijitee.I1083.0789S219.

[16] J. Hong, T. Dreibholz, J. A. Schenkel, and J. A. Hu, "An Overview of Multi-cloud Computing," in Advances in Intelligent Systems and Computing, 2019, vol. 927, pp. 1055–1068. doi: 10.1007/978-3-030-15035-8-103.

[17] S. Kathuria, 'A survey on security provided by multi-clouds in cloud computing', International Journal of Scientific Research in Network Security and Communication, vol. 6, no. 1, pp. 23–27, 2018.

[18] D. Petcu, 'Multi-cloud: expectations and current approaches', in Proceedings of the 2013 international workshop on Multi-cloud applications and federated clouds, 2013, pp. 1–6.

[19] L. Chouhan, P. Bansal, B. Lauhny, and Y. Chaudhary, "A Survey on Cloud Federation Architecture and Challenges," in Lecture Notes in Networks and Systems, vol. 100, Springer, 2020, pp. 51–65. doi: 10.1007/978-981-15-2071-6-5.

[20] R. Buyya, J. Broberg, and A. M. Goscinski, Cloud computing: Principles and paradigms. John Wiley and Sons, 2010, pp. 393-410

[21] J. Hong, T. Dreibholz, J. A. Schenkel, and J. A. Hu, "An Overview of Multi-cloud Computing," in Advances in Intelligent Systems and Computing, 2019, vol. 927, pp. 1055–1068. doi: 10.1007/978-3-030-15035-8-103.

[22] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," Information Systems, vol. 48, pp. 132-150, 2015.

[23] M. R. M. Assis, L. F. Bittencourt, and R. Tolosana-Calasanz, "Cloud federation: Characterization and conceptual model," in Proceedings - 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, UCC 2014, Jan. 2014, pp. 585–590. doi: 10.1109/UCC.2014.90.

[24] T. Kurze, M. Klems, D. Bermbach, A. Lenk, S. Tai, and M. Kunze, 'Cloud federation', Cloud Computing, vol. 2011, pp. 32–38, 2011.

[25] L. Mashayekhy, M. M. Nejad, and D. Grosu, "A Trust-Aware Mechanism for Cloud Federation Formation," IEEE Transactions on Cloud Computing, vol. 9, no. 4, pp. 1278–1292, 2021, doi: 10.1109/TCC.2019.2911831.

[26] D. Villegas et al., "Cloud federation in a layered service model," in Journal of Computer and System Sciences, 2012, vol. 78, no. 5, pp. 1330–1344. doi: 10.1016/j.jcss.2011.12.017.

[27] M. A. Salehi, A. N. Toosi, and R. Buyya, "Contention management in federated virtualized distributed systems: implementation and evaluation," Software: Practice and Experience, vol. 44, no. 3, pp. 353-368, Mar. 2014.

[28] H. A. Imran et al., 'Multi-cloud: a comprehensive review', in 2020 IEEE 23rd International Multitopic Conference (INMIC), 2020, pp. 1–5.

[29] A. N. Toosi, R. N. Calheiros, R. K. Thulasiram, and R. Buyya, "Resource provisioning policies to increase IaaS provider's profit in a federated cloud environment," in Proc.- 2011 IEEE International Conference on HPCC 2011, pp. 279–287. doi: 10.1109/HPCC.2011.44.

[30] M. Singhal, S. Chandrasekhar, T. Ge, R. Sandhu, R. Krishnan, G. J. Ahn, and E. Bertino, "Collaboration in multicloud computing environments: Framework and security issues," Computer, vol. 46, no. 2, pp. 76-84, Feb. 2013.

[31] T. Diaby and B. B. Rad, "Cloud Computing: A review of the Concepts and Deployment Models," International Journal of Information Technology and Computer Science, vol. 9, no. 6, pp. 50–58, Jun. 2017, doi: 10.5815/ijitcs.2017.06.07.

[32] L. Savu, "Cloud computing: Deployment models, delivery models, risks and research challanges," in 2011 International Conference on Computer and Management, CAMAN 2011, 2011. doi: 10.1109/CAMAN.2011.5778816.

[33] W. Jansen and T. Grance, "Guidelines on security and privacy in public cloud computing," Gaithersburg, MD, 2011. doi: 10.6028/NIST.SP.800-144.

[34] P. Hofmann and D. Woods, "Cloud computing: The limits of public clouds for business applications," IEEE Internet Comput, vol. 14, no. 6, pp. 90–93, Nov. 2010, doi: 10.1109/MIC.2010.136.

[35] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1. pp. 69–73, Jan. 2012. doi: 10.1109/MIC.2012.14.

[36] S. Islam, M. Ouedraogo, C. Kalloniatis, H. Mouratidis, and S. Gritzalis, "Assurance of Security and Privacy Requirements for Cloud Deployment

 ISBN: 978-1-68558-044-5

Models," IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 387–400, Apr. 2018, doi: 10.1109/TCC.2015.2511719.

[37] T. Guo, U. Sharma, P. Shenoy, T. Wood, and S. Sahu, "Cost-aware cloud bursting for enterprise applications," in ACM Transactions on Internet Technology, 2014, vol. 13, no. 3. doi: 10.1145/2602571.

[38] V. Viji Rajendran and S. Swamynathan, "Hybrid model for dynamic evaluation of trust in cloud services," Wireless Networks, vol. 22, no. 6, pp. 1807–1818, Aug. 2016, doi: 10.1007/s11276-015-1069-y.

[39] J. Abawajy, 'Establishing trust in hybrid cloud computing environments', in 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, 2011, pp. 118–125.

[40] C. Lin and V. Varadharajan, 'A hybrid trust model for enhancing security in distributed systems', in The Second International Conference on Availability, Reliability and Security (ARES'07), 2007, pp. 35–42.

[41] A. Marinos and G. Briscoe, 'Community cloud computing', in Cloud Computing: First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009. Proceedings 1, 2009, pp. 472–484.

[42] F. Liu et al., 'NIST cloud computing reference architecture', NIST special publication, vol. 500, no. 2011, pp. 1–28, 2011.

[43] A. Elhabbash, F. Samreen, J. Hadley, and Y. Elkhatib, "Cloud brokerage: A systematic survey," ACM Computing Surveys, vol. 51, no. 6. Association for Computing Machinery, Jan. 01, 2019. doi: 10.1145/3274657.

[44] A. Ghorbel, M. Ghorbel, and M. Jmaiel, 'Privacy in cloud computing environments: a survey and research challenges', The Journal of Supercomputing, vol. 73, no. 6, pp. 2763–2800, 2017.

[45] T. Halabi and M. Bellaiche, "A broker-based framework for standardization and management of Cloud Security-SLAs," Comput Secur, vol. 75, pp. 59–71, Jun. 2018, doi: 10.1016/j.cose.2018.01.019.

[46] H. AlJahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, and J. Xu, 'Multi-tenancy in cloud computing', in 2014 IEEE 8th international symposium on service oriented system engineering, 2014, pp. 344–351.

[47] R. Kumar, S. · Jitendra, A. · Sanjeev, S. · Narendra, S. Chaudhari, and · K K Shukla Editors, "Lecture Notes in Networks and Systems 100." [Online]. Available: http://www.springer.com/series/15179

[48] K. Bernsmed, M. G. Jaatun, P. H. Meland, and A. Undheim, "Thunder in the Clouds: Security challenges and solutions for federated Clouds," in CloudCom 2012 - Proceedings: 2012 4th IEEE International Conference on Cloud Computing Technology and Science, 2012, pp. 113–120. doi: 10.1109/CloudCom.2012.6427547.

[49] P. Arias Cabarcos, F. Almenárez, F. Gómez Mármol, and A. Marín, "To federate or not to federate: A reputation-based mechanism to dynamize cooperation in identity management," Wirel Pers Commun, vol. 75, no. 3, pp. 1769–1786, Apr. 2014, doi: 10.1007/s11277-013-1338-y.

[50] P. Arias-Cabarcos, F. A. Rez-Mendoza, A. Marín-López, D. Díaz-Sánchez, and R. Sánchez-Guerrero, "A metric-based approach to assess risk for 'On cloud' federated identity management," Journal of Network and Systems Management, vol. 20, no. 4, pp. 513–533, Dec. 2012, doi: 10.1007/s10922-012-9244-2.

[51] M. Ogawa and L. Xin, "Proxy Certificate Trust List for Grid Computing Time-Sensitive Pushdown Systems View project Proxy Certificate Trust List for Grid Computing." [Online]. Available: https://www.researchgate.net/publication/252163600. Accessed: March 2, 2023.

[52] V. Radha and D. H. Reddy, "A Survey on Single Sign-On Techniques," Procedia Technology, vol. 4, pp. 134–139, 2012, doi: 10.1016/j.protcy.2012.05.019.

[53] E. Maler et al., 'Security and privacy considerations for the oasis security assertion markup language (saml) v2. 0', Language (SAML), vol. 2, p. 0, 2005.

[54] C. Mainka, V. Mladenov, J. Schwenk, and T. Wich, "SoK: Single Sign-On Security - An Evaluation of OpenID Connect," in Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS and P 2017, Jun. 2017, pp. 251–266. doi: 10.1109/EuroSP.2017.32.

[55] H. Gomi, "Dynamic identity delegation using access tokens in federated environments," in Proceedings - 2011 IEEE 9th International Conference on Web Services, ICWS 2011, 2011, pp. 612–619. doi: 10.1109/ICWS.2011.30.

[56] M. Ghasemisharif, A. Ramesh, S. Checkoway, C. Kanich, J. Polakis, and A. Ramesh, Open access to the Proceedings of the 27th USENIX Security Symposium is sponsored by USENIX. O Single Sign-Off, Where Art Thou? An Empirical Analysis of Single Sign-On Account Hijacking and Session Management on the Web O Single Sign-Off.

[57] C. Gentry, A fully homomorphic encryption scheme. Stanford university, 2009.

[58] R. Gallon, M. Holanda, A. Araújo, and M. E. Walter, 'Storage policy for genomic data in hybrid federated clouds', in Advances in Bioinformatics and Computational Biology: 9th Brazilian Symposium on Bioinformatics, BSB 2014, Belo Horizonte, Brazil, October 28-30, 2014, Proceedings 9, 2014, pp. 107–114.

[59] M. Rosa et al., "BioNimbuZ: A federated cloud platform for bioinformatics applications," in Proceedings - 2016 IEEE International Conference on Bioinformatics and Biomedicine, BIBM 2016, Jan. 2017, pp. 548–555. doi: 10.1109/BIBM.2016.7822580.

[60] C. A. L. Borges, H. v. Saldanha, E. Ribeiro, M. T. Holanda, A. P. F. Araujo, and M. E. M. T. Walter, "Task scheduling in a federated cloud infrastructure for bioinformatics applications," in CLOSER 2012 - Proceedings of the 2nd International Conference on Cloud Computing and Services Science, 2012, pp. 114–120. doi: 10.5220/0003932801140120.

[61] A. P. Heath et al., "Bionimbus: A cloud for managing, analyzing and sharing large genomics datasets," Journal of the American Medical Informatics Association, vol. 21, no. 6, pp. 969–975, Jan. 2014, doi: 10.1136/amiajnl-2013-002155.

[62] D. Lima et al., "A storage policy for a hybrid federated cloud platform: A case study for bioinformatics," in Proceedings - 14th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing, CCGrid 2014, 2014, pp. 738–747. doi: 10.1109/CCGrid.2014.102.

[63] H. H. D. P. M. Costa, A. P. F. de Araújo, J. J. C. Gondim, M. T. de Holanda, and M. E. M. T. Walter, "Attribute based access control in federated clouds: A case study in bioinformatics," in 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1-7, June 2017.

[64] H. Saldanha et al., "Towards a Hybrid Federated Cloud Platform to Efficiently Execute Bioinformatics Workflows," in Bioinformatics, InTech, 2012. doi: 10.5772/50289.

[65] B. Langmead, K. D. Hansen, and J. T. Leek, "Cloud-scale RNA-sequencing differential expression analysis with Myrna," 2010. [Online]. Available: http://genomebiology.com/content/11/8/R83

[66] C. Hoffa et al., "On the use of cloud computing for scientific workflows," in Proceedings - 4th IEEE International Conference on eScience, eScience 2008, 2008, pp. 640–645. doi: 10.1109/eScience.2008.167.

[67] D. P. Wall, P. Kudtarkar, V. A. Fusaro, R. Pivovarov, P. Patil, and P. J. Tonellato, "Cloud computing for comparative genomics," 2010. [Online]. Available: http://www.biomedcentral.com/1471-2105/11/259

[68] R. Li et al., "SNP detection for massively parallel whole-genome resequencing," Genome Res, vol. 19, no. 6, pp. 1124–1132, Jun. 2009, doi: 10.1101/gr.088013.108.

[69] B. Pratt, J. J. Howbert, N. I. Tasman, and E. J. Nilsson, "Mr-Tandem: Parallel x!Tandem using Hadoop MapReduce on Amazon web services," Bioinformatics, vol. 28, no. 1, pp. 136–137, Jan. 2012, doi: 10.1093/bioinformatics/btr615.

[70] L. Zhang, S. Gu, Y. Liu, B. Wang, and F. Azuaje, "Gene set analysis in the cloud," Bioinformatics, vol. 28, no. 2, pp. 294–295, Jan. 2012, doi: 10.1093/bioinformatics/btr630.

[71] B. Lang, I. Foster, F. Siebenlist, R. Ananthakrishnan, and T. Freeman, "A flexible attribute based access control method for grid computing," J Grid Comput, vol. 7, no. 2, pp. 169–180, 2009, doi: 10.1007/s10723-008-9112-1.

[72] M. Najam, R. U. Rasool, H. F. Ahmad, U. Ashraf, and A. W. Malik, "Pattern Matching for DNA Sequencing Data Using Multiple Bloom Filters," Biomed Res Int, vol. 2019, 2019, doi: 10.1155/2019/7074387

[73] M. Akgün, A. O. Bayrak, B. Ozer, and M. Ş. Sağiroğlu, "Privacy preserving processing of genomic data: A survey," Journal of Biomedical Informatics, vol. 56. Academic Press Inc., pp. 103–111, Aug. 01, 2015. doi: 10.1016/j.jbi.2015.05.022

[74] S. Simmons, C. Sahinalp, and B. Berger, "Enabling Privacy-Preserving GWASs in Heterogeneous Human Populations," Cell Syst, vol. 3, no. 1, pp. 54–61, Jul. 2016, doi: 10.1016/j.cels.2016.04.013.

[75] S. Sharma and A. Kaul, "A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud," Vehicular Communications, vol. 12. Elsevier Inc., pp. 138–164, Apr. 01, 2018.

[76] K. Sarwar, S. Yongchareon, J. Yu, and S. Ur Rehman, "A Survey on Privacy Preservation in Fog-Enabled Internet of Things," ACM Comput Surv, vol. 55, no. 1, pp. 1–39, Jan. 2023, doi: 10.1145/3474554.

[77] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," Vehicular Communications, vol. 16. Elsevier Inc., pp. 45–61, Apr. 01, 2019. doi: 10.1016/j.vehcom.2019.02.002.

 ISBN: 978-1-68558-044-5