Privacy and Security Enhancement in Multi Cloud Architecture

Ashwini G. Sharma
Department of Computer Science and Engineering
MGICOET,
Shegaon(Maharashtra)
ashwini.unnati@gmail.com

Animesh Tayal
Department of Computer Science and Engineering
Priyadarshini College of engineering and technology,
Nagpur(Maharashtra)
annu09in@gmail.com

***Abstract*—**When considering the adoption of cloud services, security challenges are still among the biggest obstacles. The various cloud security threats targeting resulting in a volume of proposals, a lot of research activities has begun. Along with these security issues, cloud security paradigm novel approaches, techniques, and open the way towards architecture, which comes with a new set of unique features. The paper obtained by using multiple different clouds provides a survey on security merits. Several specific architecture according to their security and privacy capabilities and possibilities are introduced and discussed.

*****

I. INTRODUCTION(1)

Cloud computing provides dynamically scalable resourcesProvision as a service over the Internet. Thirdparty,On-demand, self-service, pay per core for use, andBy offering scalable computing resources and servicesWith cloud pattern promise to reduce capitalOperating expenses for hardware and software.Clouds can be classified to the physical locationFrom the user's point of view into account [1]. a publicCloud is offered by third party service providers andThe user of the premises, including outside resources. in situationCloud systems typically installed at the user's premisesIts data center, private cloud is called the setup. EThe hybrid approach is marked as hybrid cloud. This paper willTo focus on public clouds due to these serviesThe highest security requirements, but also-as the demand forThis paper will start in the debate included high capacitySecurity prospects.Public cloud, in all of the three common cloud serviceLayers (IaaS, Paas, SaaS) that share similaritiesEnd-users' digital assets are taken from a intraorganizationalFor an interorganizational context. This creates aThe number of issues, among which security aspects
Regarded as the most important factor when consideringCloud computing adoption [2]. Legislation and complianceFurther challenges to the increased outsourcing arrangementsData, applications, and processes. High Privacy StandardsThe EU, as such, and their legal forms
Especially between the countries of the continent give rise toTechnical and organizational challenges [3].Data and applications to reduce the risk of an ideaA public cloud is used with many ofcloud. This model employs several approachesRecently been proposed. They differ in the division andDistribution pattern, technology, cryptographic methods,And the case of the security level targeted. This paper[4] is an extension of and these include a survey onmulticloud adopting different approaches to security. ThisMulticloud halfhearted offers four different modelsArchitecture. The architecture developed multicloudAvailable plans and allow to classifyAnalyze them according to their safety benefits. OneWith regard to the legal assessment of different waysCompliance aspects and implications especially given.The rest of this paper is organized as follows: section 2 The need for effective cloud security countermeasures inspire. Briefly review the current state of play. Further observations lead to the fact that most of the Research and development work is currently devoted to Do not consider the dedicated protection schemes,the specific properties of clouds. Recently somemaking use of several different clouds on the proposal To realize the goals of security at the same time started to appear. To Classifying and analyzing these to provide a formal groundProposals, we propose a set of four different multicloudArchitecture. These architectures are introduced multicloudEach of them discussed further in Section 3 and is Including case studies Section 4, 5, 6, and 7. Section 8 Legal and compliance aspects of the idea. Finally, section 9, and an assessment of the
The approach is presented.

II. CLOUD SECURITY ISSUES

These issues range from essential Confidence in the cloud provider and cloud interfaces attack For attacks on other systems to abuse cloud services. The main problem is that the cloud computing paradigm Includes secure sourcing of indirect sensitive As well as business-critical data and processes. When Consider using a cloud service, users must be aware All data up to the cloud provider is the fact that Self-control and security. Even more, if deployment (IaaS or pass-through) for cloud data processing applications, A cloud providers gain full control over these processes. Therefore the cloud, a strong trust relationship Provider and cloud user is considered a normal Cloud computing condition. This faith can touch depends on the political context Legal liability. For example, Italian law requires Italian citizens that the official data, if collected by Government agencies, is to remain in Italy. Thus, using One out of Italy for the realization of a cloud provider Italian citizens will be provided in the e-government service This obligation is violated immediately. Therefore, cloud users Must rely on their data hosted within the cloud provider And copy them to the borders of the country ever Or for backup in case the country also closed position (Local failure) nor the institutions for providing data access From

abroad. That an attacker access to cloud storage Component in taking photos or alter data is Storage. This is often done once, or may be Constant. It also has access to an attacker Clouds can modify the function of the processing logic And their input and output data. even although In most cases it may be legitimate to assume a cloud Providers can be honest and clients' cases to deal with A respectful and responsible manner, there still remains a The threat of malicious employees of cloud providers, successful Or attacks by third parties and compromisation Orders processed by a summons. Security flaws and attacks on cloud [6], in an overview infrastructures are. Some more recent examples Advances are briefly discussed in the following. Ristenpart and others. [7], [8] presented some attack techniques Amazon EC2 IaaS service virtualization. Their Approach, the attacker until the allocation of new virtual machines As a sufferer runs on the same physical machine machine. However, the attacker can perform cross-VM sidechannel Learn attacks or victims to modify data. The authors present strategies for reaching the desired target Machine with a high probability, and how to exploit show Confidential data, such as the position of the extractCryptographic key from the victim's VM ,. Finally, they Cross- VM technology to fend off proposed the use of blinding Side-channel attacks. Amazon in the management interface [9], a defect in EC2 was found. SOAP uses XML-based interface Signatures for integrity protection is defined as WS- Security Verification and authenticity. Gruschka and Iacono [9] Turns out that the implementation of EC2 for signature Wrapping signature verification is vulnerable to attack [10]. In this attack, an attacker who eavesdropped Legitimate requests messaging can add another arbitrary Keeping Operations original messageSignature. Due to defects in the structure of EC2, The ame ndment does not address the message and injection The operation is executed on behalf of legitimate users and Billed to the account of the victim. In a SaaS cloud was in 2009 with a major event Google Docs [11]. Google Docs allows users to edit Documents (eg, text, spreadsheet, presentation) online And share documents with other users. However, this The system had the following defects: a document once Shared with anyone, it was accessible to all The document owner is ever shared with the documents. For the technical malfunction, was not any criminal intent Is necessary to gain unauthorized access to confidential data. Recent attacks have demonstrated that the cloud systems The major cloud providers may be serious security flaws Different types of clouds (see [12], [13]). Related work can be seen on this review: Cloud system attacks, cloud computing paradigm There is an inherent risk of working in a settlement Cloud system. An attacker is able to infiltrate cloud The system itself, all data and processes of operating all users The cloud system may be subject to malicious An avalanche manner action. Therefore, cloud computing Paradigm requires an in-depth rethink whatSecurity requirements may be affected by such an exploit

Event. For the common case of a single cloud provider Hosting and processing of user data, an intrusion Immediately affects the security requirements: Reach, Integrity, and confidentiality of data and procedures, May be violated, and further action may be malicious Cloud performed by the user's identity. The cloud security issues and trigger a lot of challenges Research activities, resulting in a volume of proposals Cloud security threats targeting different. Together These safety issues, a new model comes with cloud Set of unique features that open the way to novel Safety perspective, technology, and architecture. OnePromising concept uses several different clouds Together.

III. SECURITY PROSPECTS BY MULTICLOUD ARCHITECTURES

The basic underlying idea is to use several different clouds At the same time to minimize the risk of malicious data Manipulation, disclosure, and manipulating the process. By Different clouds, integrating faith belief may be noncollaborating lowered to a notion of cloud service Providers. In addition, this setting makes it very difficult one External attacker to retrieve or manipulate data to the host or A typical user of cloud applications. The idea to use multiple clouds Has been proposed by Bernstein and Celestia [14], [15]. However, none of the work yet has focused on security. Since then, other approach has to consider the security implications that are proposed. These methods are working on different Cloud service levels, partly are combined with cryptographic Methods, and targeting different usage scenarios. In this paper, we present a different model architecture patterns for the distribution of resources for multiple cloud providers. This model is used to discuss security benefits and also to classify existing approaches,

In our model, we can distinguish the following four architectural patterns ::

1) Replication application can receive multiple results of an operation in different Clouds and compare within the premise own (see Section 4). This allows the user to obtain a evidence of the integrity of the result.

2) Partition system allows application levels separate the logic of the data (see Section 5). Is It gives additional protection against data leaks due failures in the application logic.

3**) Allows partitioning of application logic** into pieces Different cloud application logic delivery (See Section 6). This has two advantages. First, no clouds Provider learns entire application logic. Second, a cloud provider overall learning The application calculates the result. Thus, this leads Data and application privacy.

4) The fragment allows **partitation of application data** into piecesThe fine-grained pieces of data distribution Different clouds (see section 7). None of the involved All data which cloud providers gain access Protect the confidentiality of data.

Provides architectural patterns appear every Various processes which map to the individual merits protection, Views and need protection. Obviously, Patterns of residential security can be combined results Merits, but it also seeks more diplomats and runtime. The following section presents four patterns And details with respect to the evaluation of their merits and flaws

Under the concept of security requirements called One or more compromised cloud system.

IV. REPLICATION OF APPLICATION

How does a cloud customer know whether his data were processed correctly within the cloud? There is no technique how to ensure that an operation in a cloud system was not manipulated or that the cloud system was not compromised by

an attacker. The only type of guarantee is based on the level of trust between the cloud customer and the cloud provider and the contractual made including regulations such as the SLA applicable laws and regulations of the jurisdiction involved domains. But even if the relationship and agreements are fully respected by all participants, there is still a residual risk of being compromised by others.

To resolve this intrinsic problem, multiple different clouds run multiple copies of the same application can be displayed (see Fig. 1). Instead of running a particular application specific cloud, the same operation is executed by different clouds. By comparing the obtained results, the user obtains evidence cloud integrity result. In that environment, the necessary confidence to the cloud service provider can be drastically reduced. Instead of trusting a service provider cloud completely, the user only needs to trust the cloud assumption that cloud providers do not cooperate maliciously against itself.

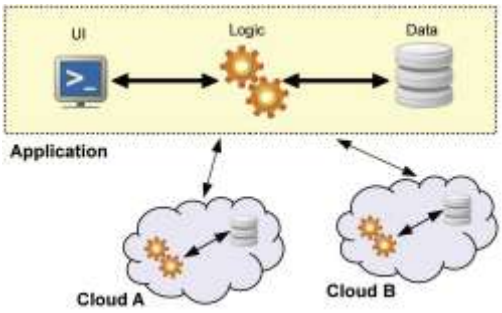

Fig. 1. Replication of application systems.

Let us consider that n > 1 clouds are available (shown in fig as Clouds A and B for example). All adopted n clouds perform the same task. Suppose further that f indicates the number of malicious clouds and n? f> f most Clouds are honest. The result may be correct, then cloud user obtained by comparing the results and as having the most correct. no other methods of deriving the correct result, for example, using TurpinCoan algorithm [16] to solve the general Byzantine agreement problem.
Instead of performing cloud user Verification work, are involved in a more efficient access More clouds oversee implementation of a cloud. To For example, Cloud could be a declaration of intermediate results of its To run a monitoring program associated calculations Claude B. In this way, Cloud B can verify that a Cloud Progress and the number of sticks Cloud user. An extension of this approach, as Cloud B That is certified to run can run a model checker service Allowing for instant on-the-fly Cloud, a path taken, Detection of irregularities.
This architecture allows checking the integrity of the results obtained from the tasks deployed in the cloud. On the other side, we note that provides no protection with regard to confidentiality of the data or processes. By contrast, this approach could have a negative impact on confidentiality because-due to the multi-cloud deployment raises the risk that one of they are malicious or compromised. To implement protection against unauthorized access to data and logic of this architecture needs to be combined with the architecture It described in Section 5.
The idea of resource replication can be found in many other disciplines. In the design of reliable systems, example, is used to increase system robustness especially against system failures [17]. In the financial business processes-and especially in the management of providers supply chains one code are avoided reduce dependence on suppliers and increase flexibility of business processes [18]. In all these cases, the additional overhead introduced by doing multiple things Sometimes that was accepted in favor of other objectives resulting from this replication.
The architectural concept can be applied to all three Cloud layer. Saas-layer is discussed in a case study Section 4.1.

Imagine a cloud provider that called InstantReporting It offers the service of creating annual financial reports automatically out of a given set of business data. This is a very typical scenario of use of the cloud, as the Report It must be published by all business entities once a year. Therefore, the resources needed to create such reports are It is only necessary for a small period of time each year. So, using a cloud service for it third in the house resources can be omitted, which would be the idler year. On the other side, by sharing its service capabilities among a large group of companies, all of which have to create their reports at different times of year, a cloud service You get great benefits provider to provide such shared service "in the cloud".
However, as promising as this scenario seems to be in terms of use of the paradigm of cloud computing, which contain a fundamental flaw: The cloud customers can not verify that The annual report created by the cloud service is correct. There could have been accidental or intentional changes of the source data for the report, or processing logic that creates reports on the strength of source data contain errors. In the worst case, the system itself was cloud compromised (eg, by a malicious competitor) and all Reports are slightly modified so that they look conclusive but they contain slightly reduced profit margins, aimed at You make a competitor look bad, or even insolvent.

4.1.1 Dual Execution
In such a situation, first and trivial approach to verification could be a client causes the cloud creating an annual report accounting more than once. For example, instead of giving the same request to one the only cloud provider (called Cloud A hereafter), a second cloud provider (called Cloud B) that provides an equivalent type of service is invoked in parallel. By placing the same Clouds petition A and B, a user can immediately cloud identify if your request was processed differently Clouds A and B. Therefore, in this way, a secret operating either side service application would be detected. However, besides the costs double the investment thereof application twice, this approach is also based on existence of at least two different cloud provider with and offers equivalent services comparable type of the result. Depending on the type of cloud resources used, this is either easy as if even today already the many different cloud providers that offer equivalent services (See Section 1), or difficult in cases where very specific resources are demanded.

4.1.2 n Clouds Approach
A more advanced approach, but also more complex comes discipline of distributed algorithms: Byzantine Protocol Agreement. N assume the existence of cloud suppliers, of which collaborate f against maliciously User cloud with n> 3f. In that case, each of the n clouds It performs the task of calculation proposed by the user in the cloud. Then, all cloud providers run a distributed collaborative algorithm that solves the general Byzantine Agreement problem (eg TurpinCoan [16] or Exponential information Collection [19], algorithms 6.2.3). After ensures all suppliers not know the correct malicious cloud calculation result. Therefore, in the final stage, the result the user communicates through the cloud safe Diffusion algorithm (eg flood plain, with the cloud user having the most as a result). Therefore, the user cloud You can determine the correct result, even in the presence of malicious clouds f.

4.1.3 Processor and Verifier
Instead of putting Clouds A and B perform the same application, another feasible approach is to have one cloud provider "Monitor" for the execution of another cloud provider. For example, A can announce intermediate Cloud results of its calculations to a career monitoring process Cloud B. In this way, the cloud B can verify A cloud It makes progress and sticks to the computer provided by the cloud customer. As an extension of this approach, B can run a cloud service models tester check execution path taken by the cloud on the fly, allowing immediate detection of irregularities.
One of the main benefits of this approach is its flexibility. Cloud B does not have to know all the details of the Lead time cloud A-especially not on the data processed values, but is able to detect and report anomalies cloud customer immediately. However, the guarantees offered by this approach depend strongly on the type, number and verifiability of intermediate results given the cloud B.

V. PARTITION OF APPLICATION SYSTEM INTO TIERS

The architectural pattern described in section 4 above It allows the user to cloud to get some evidence about the integrity calculations of the resources of a third party or services.
The architecture introduced in this section is directed wing risk of unwanted data leakage. Answer the question on Cloud how a user can be sure that access to data is implemented and effectively enforced and that errors in the application logic does not affect user data?
In order to limit the risk of data leakage due to unwanted Application logic errors, different applications Level clouds clear and the system of their delegation Proposed (Fig. 2 for details). In the case of failure of the application, It is not immediately at risk from actual data Protected by access control and separation of independent Plan. Moreover, the choice to select a cloud user Perhaps the reliable provider of cloud-specific Cloud storage service providers and other data Applicatio./
It should be noted that the security services provided by this architecture it can only be fully exploited if the It is done executing the application logic on data system in the cloud user. Only in this case, the application provider learns nothing in the user data. So, delivering a request to the user side in SaaS-based with controlled access to user data access It made from the same system user is the most far-reaching instantiation.

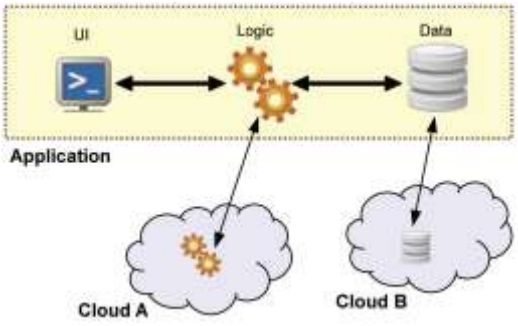

Fig. 2. Partition of application system into tiers.

In addition to the overhead introduced by the addition cloud involved, this architecture requires, moreover, standardized interfaces for applications with data pair services provided by different parties. Also generic data services may serve a wide range of applications there It will be the need for specific application services as well.
The division of systems and application levels the distribution of clouds of varying levels provides some coarse protection against data leakage in the presence of design flaws or application execution. this architecture concept can be applied to all three layers of clouds. In The next section, a case study in the SaaS-layer is discussed.

5.1 Case Study
Taking SaaS-based service called PhotOrga that It allows its users to upload and manage your photos and and share with family, friends and other contacts. For this purpose, it provides convenient access PhotOrga control system. In this environment, how can the user be sure This access control system is implemented correct and effective? Since the application logic and the data storage system are closely PhotOrga integrated a flaw in the logic of the application can have side effects on controlling access to the photos. This could result in unwanted data leakage (as in Google Docs case referred to in Section 2).
persistence layer with the assignment of two different clouds reduces the risk of data leakage in the presence of application logical flaws. Since the data are not directly accessible by the applications, design or programming errors in the application They are not as widespread as in effect
integrated scenario.
From a viewpoint of implementation, this can be performed by OAuth. When the application (in the cloud) You want to access a photo creates demand for OAuth and redirects the user to the storage provider (cloud B). the user is asked to grant or refuse this authorization petition. In this way, the user gains more control over their data while a slightly higher management effort.
This scenario can be extended to a host of other services including email, documents, spreadsheets, and so on.

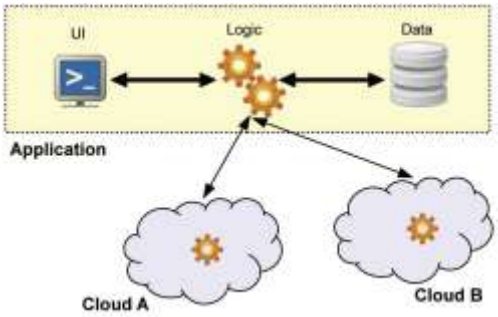

Fig. 3. Partition of application logic into fragments.

VI. PARTITION OF APPLICATION LOGIC INTO FRAGMENTS

This variant architecture addresses the confidentiality of data and processing logic. A response is given to the following Question: How can a user to avoid the cloud fully disclose or data processing logic to the cloud provider? The data should not only be protected, while the persistent storage, but particularly when it processed.

The idea of this architecture is that the logic of the applicationYou need to be divided into parts and these fine-grained parts are distributed to various clouds (see Fig. 3). Is approach can be instantiated in different ways depending on how the partition is made. Clouds participate in fragmented applications may be symmetrical or asymmetric in terms of computing power and confidence. Two concepts are common. The first consists of a Private cloud of confidence leading to a small critical part of the computing, and a public cloud is not trusted that takes more the computational load. The second distributes counting between several public clouds are not trustworthy,It is assuming that these clouds are not colluding to break safety.

6.1 Obfuscating Splitting

By this approach, engaging portions are distributed so different clouds, each cloud has only a partial view of the application and only profits limited knowledge. Therefore, this method can also hide parts of the application logic clouds. By enforcement division, a first approach is to use the existing sequential or parallel logic separation. Thus, depending on the application, each cloud provider simply makes subtasks in a subset of data.

An approach Danezis and Livshits [20] is the accumulation around a storage architecture confident and focused online the provision of services, where the service depends on the result of function evaluations of user data. IsIt proposed using the cloud as secure storage, with the keys Remaining on the client side, for example, in a private cloud. the application is divided as follows: The service sends the function to be evaluated for the customer. The client retrieves necessary raw data and processes it according to the service needs. The test result and a correction is given back to the provision of public cloud service. In the cloud, the remaining functionality of the service offered based on aggregate customer input. this architecture Detailed protects user data, and reveals just what the cloud need to know to provide the service.////

Similarly, the FlexCloud [21] approach is based on the interconnection , Private local computing environments to a semitrusted public cloud for the realization of complex workflows or secure distributed storage. This approach uses multiple secure computing environments with limited resources ("Private clouds") to form a collaborative computing community environment similar level of trust, a reliable " cloud."////

A difficult challenge is generally obscure division the fact that no generic pattern for realization. Careful consideration where the application can be divided into fragments must be made with regard to its confidentiality, ie check whether the information cloud participate providers are really harmless.

6.2 Homomorphic Encryption and Secure Multiparty Computation

Homomorphic encryption and secure multiparty computationboth they use cryptographic means to protect data whileIt is processed. In homomorphic encryption, the user encrypts data with your public key and load ciphertexts to the cloud. The cloud can independently calculating in the encrypted data to obtain an encrypted result that only the user can decrypt. Therefore, in our scenario, the homomorphic encryption uses an asymmetrical fragmentation, where the user (or a small private trust cloud) manages and performs encryption keys and decryption operations while the mass calculation data is encrypted by a public cloud is not trusted.//

The possibility of fully homomorphic encryption support In addition multiplication safe and ciphertextsIt was first suggested in [22]. However, long all known homomorphic encryption schemes supported efficiently one operation [23], [24]. Therefore, recent discovery of fully homomorphic encryption by Gentry [25] Asharov et al. [26] had a tremendous impact on the cryptographic research community and revived in this field.

For homomorphic encryption, the cloud has the the main share of the work as it operates in the coded entries to calculate the encrypted output. However, algorithmsThey are far from practical, so the view of clouds based on homomorphic encryption seems unreal to the next future. Moreover, the applicability is limited to services that go beyond the outsourcing of computing, intermediate or final results need to be deciphered. Is or it requires interaction with the entity that holds the key (for example, a private cloud) or the key is shared among several clouds then help decipher values needed clear a threshold encryption scheme [27].

The idea was first secure multiparty computation presented in [28] as a solution to millionaire problem: Two millionaires want to know who is richer without disclose any further details about their wealth. Two insurance main variants are known multiparty computation: Based on the linear reciprocating secret [29] or confusing circuits [30]. Schemes based on a work-sharing scheme linear secrets as follows: The user calculates and distributes the shares of the different clouds. Clouds count together the the function of the interests of these actions, communication with each other when necessary. In the end, the clouds have actions sends the results back to the user which can reconstruct the result. At least three clouds are necessary this system and no two of them to collude. The approach unreadable circuit operates as follows: A cloud generates a circuit that is capable of calculating figure desired

function and producing a circuit illegible circuit, which however remains executable. So this Cloud helps users to encrypt their input accordingly. Another cloud now need to be present to evaluate the circuit with user input. Therefore, this system requires Generally only two clouds. Although the ideas of multiparty computer are old, is ongoing research to reduce multiparty computation overhead. Recent improvements, for example, equality and comparison of values, has lead to the construction of programming frameworks, which and practice can be considered [31], [32].

An example architecture using circuits is confusing TwinClouds approach [33], which uses a private cloud preparation of unreadable circuits. The circuit itself is then evaluated within a cloud commodity High Performance lower confidence without reducing security guarantees for processes outsourced to the public cloud.

In all cases, the use of secure computing in multiparty various clouds guarantees the confidentiality of data entry, unless the cloud providers collude to open shares or decrypt tickets. Assuming that the cloud provider itself is not malicious, but it could be compromised by attacks or have malicious individual employees, that collusion is difficult set so as to give good protection. A multiparty calculating the clouds makes it possible to calculate a Based on the data in a way that no cloud provider learns nothing about the input or output.

6.3 Case Studiies

With secure multiparty computation, a number of participants You can calculate functions without their input values disclose any information about their individual contributions during the calculation. Here, we consider multiparty computation to be executed across multiple clouds. Safe use multiparty computation can be used to better protect the confidentiality of user data in online services available today, but also it has the potential to enable new services because today there are no user confidentiality requirements and lack of a trusted third party.

There are problems in the latter category in business today Environment: Multiple companies want to become a statistic analysis of their business data and market. The result isHe expected to help all of them; however, for obvious reasons, no corporation wants to share information with each other. Yes stakeholders can not identify a single trusted third party by all, this scenario requires multiparty computation between private clouds participating companies or outsourced to different public clouds.

An example of an application in the real world of insurance multiparty computation is an auction of sugar beet in Denmark [3. 4]. This auction is used by farmers selling their sugar beet processing company Danisco. The farmers' Entry to the auction depends on your situation and economic productivity, they do not want to reveal or competitor Danisco. Clearly, neither DaniscoHe wants to give the auction. As a trusted third party is that is not easily found, the easiest solution was to establish a multiparty computation between servers farmer union, Danisco, and a university support.

Although still in a prototype stage research, other application area of multiparty computing is the sharing Surveillance data security incidents and collaboration network monitoring of several ISPs [35]. As network monitoring and detection of attacks have fairly strict real-time requirements to be useful, this application requires highly efficient implementations of multiparty computation. Some algorithms are implemented under SEPIA [32]. A recent [36] is considering work new solutions of secret / efficiency compromise by introducing a help to support multi-server computing. the help server collects information sharing, so I could learn partial information for the calculation process, but then it can bring great increased efficiency, in particular for equal comparisons.

Another application that has been discussed is the offer chain management. In managing the supply chain, several companies that are part of a supply chain is to establish optimal supply chain. If the relevant information about the supply chain, such as the cost of production and capacity use resources and manpower, it is shared between all companies, it is possible to find the optimal supply chain that brings most profitable market for the product and, therefore, finally optimizes the benefit of all companies involved. As required Company information usually considered confidential by businesses, secure multiparty computing is a tool for calculate the optimal supply chain while maintaining entry secret data [37].

Secure multiparty computation can in principle be used the distribution of any computational task on multiple clouds. In If only one party holds data it is for privacy reasons it is not necessary to use more than two clouds, as we suppose the two clouds do not agree. This limits overcharging created by the multiparty computation. The task of creating the annual accounting report already mentioned in Section 4.1 may be an example, if in addition to the data integrity Ownership of data confidentiality is required. Especially for highly visible corporations, the accounting details It should be kept confidential. Otherwise, inside information or Are possible other effects on the market. However, due the nature of the creation of accounting report (only necessary once a year, the provider offers special software, and so on) that it might still be useful to perform this task within the cloud. In Here, the use of secret sharing and multiparty computation two cloud providers offer the required properties.

Other forms of division as non cryptographic obfuscation division is possible for many applications. by example, the calculation of earnings and expenses can be distributed two different cloud providers. these tasks You can perform independently without any significant above. In this case, the amount of the loss or gain, which usually the value is still more confidential undisclosed to cloud providers.

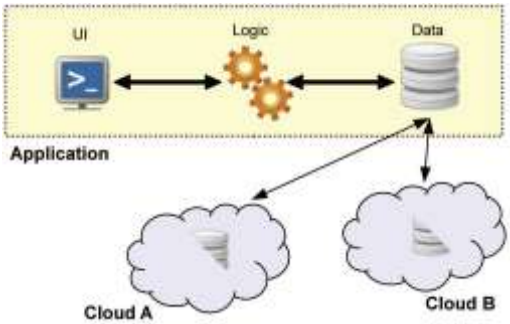

Fig. 4. Partition of application data into fragments.

VII. PARTITION OF APPLICATION DATA INTO FRAGMENTS

This multcloud architecture specifies that the application data is divided and distributed to various clouds (see Fig. 4).

The most common forms of data storage are files and database. Unstructured files typically contain data (for example, photos, text documents) and not easily allow division or exchange of parts of the data. This type of dataIt can only be partitioned using cryptographic methods (see Section 7.1). The databases contain data in structured form organized in columns and rows. Here, data partition may be performed by distributing the different parts of the database (tables, rows, columns) to various cloud providers (see Section 7.2). Finally data files may also contain structured (eg, XML data). Here, data can be separated using similar approaches as databases. XML data, for example, can be partitioned into XML element level. However, such operations are costly. Therefore, these data are more commonly treated by dividing data encryption.

7.1 Cryptographic Data Splitting

Probably the most basic method for storing data encryption safe is to store data in encrypted form. While the cryptographic key may remain on the premises of the user, increase flexibility in data processing or to allow cloud multiuser systems it is beneficial to have the key available online when necessary [38]. This approach, therefore, distributes key material and encrypted data in different clouds. For example, XML data, this may, for example, be within the XML document using XML encryption [39].

A similar approach is taken by various solutions to secure Cloud storage: The first approach to cryptographic cloud storage [40] is a solution for the encryption key / value cloud storage capacity while maintaining ease access data. It is encryption search [41], [42] as the key component for achieving this goal. encryption searchIt allows keyword search on encrypted data if an authorized Token for the keyword is provided. The keys are stored in a private cloud confidence while data residing public cloud is not trusted (see section 6.2).

An example of a relational database with encrypted Data processing is CryptDB [43]. The database consists of a database server that stores the encrypted data and a proxy who holds the keys and provides a standard SQL interface user. The data is encrypted in different layers and for the preservation schemes encryption [44], homomorphic Encryption [23], the encryption search [41], and standard symmetric encryption system, such as AES. For each SQL query, the proxy identifies and provides only the necessary keys on the server, so exactly this query you can respond. Obviously, this implies that the database Key server can learn more with each new consultation. Therefore, Persistent security against attackers is certainly limited Here. CryptDB advantage lies in the fact that the Data base portion is a standard database MySQL, and your efficiency is only marginally decreased, compared to unencrypted data storage.

Another option is to calculate a shared secret data. In a secret sharing protocol, it is not only cryptographic key involved. Instead, the secret exchange divides the data into multiple shares in such a way that data can only be rebuilt if more than a certain threshold actions are picked up. This method integrates well with multiparty calculation, as presented in Section 6.2. As discussed, multiparty computation often operates on such shares, so the clouds that form pairs of multiparty protocol can store your actions permanently without any loss of security.

7.2 Database Splitting

To protect the information within the database, you must distinguish two security objectives: confidentiality of data elements (eg a credit card number) or confidentiality of the data element relationships (for example, the articles "Peter" and "AIDS" are not confidential, but their relationship is). In the first case, the data division requires a similar scenario to other approaches presented above, with a less reliable supplier (or Additional encryption; look down). However, very often only the ratio should be protected, and this can be achieved using only honest-but-curious suppliers.

A typical way of dividing the database is of pseudonyms: A supplier receives the data with some key fields (typical personal identification data such as name, address, etc.) replaced by a random ID, and the second provider ID is allocated to the original information. This approach is used, for example, in a commercial cloud security gateway [45].

To split a database table, two General
approaches: the vertical fragmentation and horizontal fragmentation [46]. With the vertical fragmentation, columns distributed to cloud providers so that any only provider learns about his confidential relationship own. A record of patient health, for example, could be fragmented into two parts, for example, (name, patient number) and (number of patients, the disease). Thus, the individual providers only learn the relationships of noncritical data. However, for real-world applications, it is a non-trivial task to find such fragmentation. First, the new relationships can be I learned there made transitive combination Dear ones. Second, some relationships can be completed using external knowledge. If, in the above example, the first provider also learns the relationship (patient number, drug), which has technically still no knowledge about the patient's illness. However, someone with pharmaceutical background can derive the disease medication.

In addition, new relationships may also be derived by combining multiple data sets. For example, again using the relationship (patient number, medication), the knowledge of a combination of drugs can facilitate divination patient's disease. Thus, row level also, the division databaseThey may be needed. This is called horizontal fragmentation.

Finally, the database division can also be combined with encryption. The use of key management mechanisms, as mentioned before, some columns are encrypted database. the combination of encryption and protects confidential division columns and still allows database entries consultation using plain text columns

7.3 Case Study: Separation of Data Entities

As a case study for this architecture pattern multcloud one It can be considered the inverse of what to do when Data sources are federated. In many data across the organization projects federation, a common task is to harmonize different data sources prudent scheme and obtain common semantics structure. This allows a combined view in federated data. In many areas, this has been an active research and development

theme in recent years. take the data federation hospital as an example, in which different medical institutions federate their data in a particular disease, like, for example, it was the case in the research project funded by the EU celebralneurIST on aneurysms [47]. The main challenge here it is to find a way to federate data so data entities can be distributed virtually correlated.

In the pattern data partition, however, since There is a common scheme, because only one data source is at center stage. The challenge here is to find a place partition data in a way that allows to distribute the entities other than cloud data and minimize the amount of knowledge of a cloud provider can gather by analyzing the data set obtained. Therefore, it might be feasible outsource computationally intensive consultations to multicloud without violating the strict security and privacy obligations inherent in medical data (see also section 8.3.1).

VIII. LEGAL COMPLIANCE WITH MULTICLOUD ARCHITECTURES

Since the legislation faces traditionally only slowly changes technological paradigms, there are few to no cloud specific regulations in place for now. Therefore, for the cloud compute the same legal framework applies to any other means of data processing. Generally, legal compliance does not distinguish between different media technology, but rather different types of information. by example, companies face other legal requirements the legal processing of information for the prosecutor legal treatment of its Customer Relationship Management. A-all of a cloud approach not only reflects these different performance requirements.

Multi Cloud architectures can be a viable solution for companies to address these compliance issues. Therefore, this section provides a coarse grain legal analysis on the different approaches and its flaws and benefits in terms of Privacy and impact compliance.

The impending conflict between cloud computing and world of laws and policies resulting from the borders the nature of clouds in contrast to the reach of the majority legal frameworks. The most successful service in the cloud providers operate their clouds across national borders Multiple data centers worldwide. Therefore, they can not high availability even in case of failure of the region, as reduced costs due to their choice of location. In By contrast, the cloud customer is subject to their national law requirements, and faces the problem of legal guarantee compliance with national laws in a multinational environment. This conflict is not new or unique to the cloud computer, but the nature highly dynamic and virtualized clouds intensifies as the applicability of laws relating to physical location.

The legal uncertainties cloud computing, especially in Europe, with its strict data protection laws are subject to a debate. However, legal experts agree that lawful cloud computing is possible if appropriate technical, organizational and contractual safeguards for specific type of information to be processed are in place.

Before deciding on what kind of cloud services to use either public, private or hybrid, IaaS, PaaS or SaaS, the companyYou should conduct a risk assessment. This risk assessment is not only best practice, but also sometimes legally mandatory, such as a Privacy Risk Assessment Regulation of European Data Protection proposed [48]. THE proper risk assessment before the "cloud va" means identify one of the internal processes and relevant information involved in these processes, an analysis of risks and threats, and the identification of the legal requirements complianceThey have been met and the necessary guarantees to be installed. The outcome of a risk assessment of this kind might not all Company processes are suitable for a public cloud or not yet ready for the cloud.

Usually, companies processed varying types of information, having different degrees of sensitivity and need according to security checks. There may be critical for business information, requiring maximum availability, but is less critical in terms of confidentiality. Similarly, there may be given instructions for a guaranteed availability rate 99 percent is sufficient, but a violation of confidentiality It would be crucial. Legal and other compliance frameworks they can ask specific additional guarantees. For example, for processing of medical information of US citizens, a Health Insurance Portability and Accountability Act (HIPAA 1996 [49]) certification may be required. Similarly, for credit card information processing, compliance with payment Data Security Standard Card Industry (PCI DSS, [50]) is mandatory. In addition, US Federal Information Security Management Act (FISMA 2002, [51]) and US Federal Risk and Authorization Management Program (FedRAMP, [52]) relevant to the information processing of US Federal Agencies. Cloud customers based in the European Union they are hiring external cloud service providers EEA outsource processing personally identifiable information must adhere to the Data Protection Directive EU [53]. This includes mandatory for the export of personal data contractual guarantees, including mandatory contractual guarantees as Standard Contractual clauses and binding corporate rules (see [54], [55]). Moreover, many national laws require specific information to remain within national borders the country. Normally, this applies to information about national security, but also to information from public authorities or electronic health records.

Potential cloud customers face a number of them requirements for security controls, standards and certifications, probably even by varying process. Identifying one service provider cloud to offer all of these options as a Modular system seems impossible.//

Multcloud approaches can help to address these issues. As discussed below, the benefits of compliance and multicloud identified drawbacks of architectures, ingenerally it seems auspicious.//

8.1 Replication of Application

This approach appears to have fewer benefits regarding legal compliance, and multiplying the need to identify and choose a cloud service provider perfectly adapted to process requirements and relevant information. Since this could mean negotiate and conclude individual contracts with various cloud service providers, replicate a highly sensitive process or application seems unreasonably bind personal and financial means. Therefore, this approach has its value information and processes with low sensitivity but high availability and robustness requirements.

8.2 Partition of Application System into Tiers

The logical separation of data and offers the possibility of storing data in the cloud and in conformity with controls safeguards and outsource the processing logic to non-specifically certified cloud with favorable price. Also allows to store data in the cloud while the national application logic is outsourced to a multinational.

A drawback of this approach is that the compatible separation of logic and data is only possible if the application vendor does not receive customer data In any case. Treatment should be carried out in a safe environment and certified as chosen storage cloud. This can be either own customer premise a approach that almost destroys the benefits of outsourcing, reducing costs, and seamless scalability of using cloud computing, because the client needs to supply sufficient resources and fulfill itself. Alternatively, The application logic can also take place at a different level compatible cloud storage, or in a different cloud similar level of compliance. The drawback of this approach obviously, it is that the customer has to rely on clouds service providers receiving all the information, logic, and data. This somewhat contradicts the initial motivation multicloud this approach.

8.3 Partition of Application Logic/Data

8.3.1 Obfuscating Splitting and Database Splitting These approaches are particularly valuable for treating personal identification data. The segmentation of personal identification data if done in a reasonable way is a workable safeguard privacy. The best practice would be to separate the data in a way that makes the pseudonym remaining data. Pseudonyms itself is a guarantee of privacy (see [56, Section 3A]). Therefore, outsourcing pseudonymized information that is unlinkable to a specific person, does require substantial additional safeguards compared less the nonpseudonymized information.///

IX. ASSESSMENT OF MULTICLOUD ARCHITECTURES

Given the large number of specific approaches for conducting each multicloud architectures presented, is not feasible to conduct an overall assessment covering properly all of them. In addition, many approaches are only suitable in very special circumstances, making each comparison other approaches to the same domain insufficient.

However, in this section a high level is performed evaluation of all multicloud approaches presented above, focusing on their capabilities in terms of safety, feasibility, and compliance, as shown in Fig. 5. Here, security considerations suggest a general improvement approach and aggravations in terms of integrity, confidentiality, and availability of application logic or data, respectively. by eg n clouds approach is highly beneficial in terms of integrity (any deviation in execution that occurs in a single cloud provider can only be detected immediately and corrected), but rather disadvantageous in terms of confidentiality (since each cloud provider learns all on the application logic and data).

The appearance of viability on issues of applicability, business arrangement, and ease of use. Herein means the applicability flexibility to use a different approach to solve types of problems. Business-readiness assesses the extent to which research in a multicloud approach has progressed and if is ready for real-world applications, while ease of use indicates the complexity of implementing the particular Fig. 5. Evaluation and comparison of multicloud approaches. focus. For example, approaches to multi insurance calculation may be higher benefits in terms of security, but only to solve a very specific type of computing problem (ie, are limited in application), and are quite complex to implement (ie, it is not easy to use), even if they can reasonably applied.

The compliance dimension provides an indication of high the impact of each approach to legal obligations Customer implied cloud when this approach is used. Application of the approach of dual execution, for example, canIt is favorable in terms of safety and viability, but requires complex contract negotiations between cloud client and two different cloud providers, doubling the workload and obligations for all cloud request. Equivalently, the use of more than two different Cloud providers (n clouds approach) improved integrity and availability, but also it requires contract negotiations n and risk assessments, amplified by the need to assess the risks associated with automated detection and correction irregularities in n parallel executions.

Based on observations subsumed in Fig. 5, we can conclude that there is no such thing as an approach to "best". From a technical point of view, the use of multiple cloud providers leads to a perceived advantage in terms of security, based on the perception of shared-risks-and therefore mitigated. From a compliance perspective, however, many of these advantages not hold, and may even lead to further legal obligations and therefore at greater risk. The few approaches that would be beneficial in terms of security and compliance tend to be fairly limited in the viability of the application, and are not businessready however, or rather not trivial to use in real-world environments.

X. CONCLUSION

The use of multiple cloud providers to gain security Privacy and benefits is trivial. As approaches investigated in this work show clearly, no one optimal approach to promoting safe and legal compliance a omniapplicable way. Moreover, the approaches that are favorable from a technical perspective look less attractive from a regulatory point of view, and vice versa. The few approaches that score enough both these dimensions lack versatility and ease of use, therefore,It can be used in only very rare circumstances.

As it can be seen in the discussions of the four major multicloud approaches, each has its pitfalls and weaknesses, either in terms of security guarantees in terms compliance with legal obligations, or in terms of viability. Since each type of approach falls into a multicloud of these four categories, this implies a state of the art which is one therefore unsatisfactory.

However, two important signs of improvement can be taken from the tests performed in this work. First of all, given that for each type of security problem there exists at least one technical solution approach, a highly interesting field for future research lies in the combination of the approaches presented here. For example, using the n clouds approach (and assurances of integrity) in combination with sound data encryption (and assurances of confidentiality) may result in approaches that are sufficient for both technical and regulatory

requirements. We explicitly do not investigate this field here due to space constraints; However, we encourage the research community to explore these combinations, and evaluate their capabilities in terms of the dimensions proposed evaluation.
Secondly, we have identified areas of homomorphic encryption and protocols are secure multiparty computation very promising in terms of technical safety and compliance. From now on, the limitations of these approaches only derive from its close applicability and High complexity in use. However, given its excellent properties in terms of security and compliance in multicloud architectures, providing these fields to become the main building blocks for future generations of multicloud computing paradigm.

ACKNOWLEDGMENTS

It was founded work Meiko Jensen and Ninja Murnau by the European Commission, the ICT program of FP7, Contract 257 243 (TClouds Project).

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing, Version 15," Nat'l Inst. of Standards and Technology, Information Technology Laboratory, vol. 53, p. 50, http://csrc.nist.gov/groups/ SNS/cloud-computing/, 2010.

[2] F. Gens, "IT Cloud Services User Survey, pt.2: Top Benefits & Challenges," blog, http://blogs.idc.com/ie/?p=210, 2008.

[3] Gartner, "Gartner Says Cloud Adoption in Europe Will Trail U.S.by at Least Two Years," http://www.gartner.com/it/page. jsp?id=2032215, May 2012.

[4] J.-M. Bohli, M. Jensen, N. Gruschka, J. Schwenk, and L.L.L. Iacono, "Security Prospects through Cloud Computing by Adopting Multiple Clouds," Proc. IEEE Fourth Int'l Conf. Cloud Computing (CLOUD), 2011.

[5] D. Hubbard and M. Sutton, "Top Threats to Cloud Computing V1.0," Cloud Security Alliance, http://www. cloudsecurityalliance.org/topthreats, 2010.

[6] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "On Technical Security Issues in Cloud Computing," Proc. IEEE Int'l Conf. Cloud Computing (CLOUD-II), 2009.

[7] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You,
Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 199-212, 2009.

[8] Y. Zhang, A. Juels, M.K.M. Reiter, and T. Ristenpart, "Cross-VM Side Channels and Their Use to Extract Private Keys," Proc. ACM Conf. Computer and Comm. Security (CCS '12), pp. 305-316, 2012.

[9] N. Gruschka and L. Lo Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited," Proc. IEEE Int'l Conf. Web Services (ICWS '09), 2009.

[10] M. McIntosh and P. Austel, "XML Signature Element Wrapping Attacks and Countermeasures," Proc. Workshop Secure Web Services, pp. 20-27, 2005.

[11] J. Kincaid, "Google Privacy Blunder Shares Your Docs without Permission," TechCrunch, http://techcrunch.com/2009/03/07/huge-google-privacy-blunder-shares-your-docs-withoutpermission/,2009.

[12] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "All Your Clouds Are Belong to Us: Security Analysis of Cloud Management Interfaces," Proc. Third ACM Workshop Cloud Computing Security Workshop (CCSW '11), pp. 3-14, 2011.

[13] S. Bugiel, S. Nu¨ rnberger, T. Po¨ppelmann, A.-R. Sadeghi, and T. Schneider, "AmazonIA: When Elasticity Snaps Back," Proc. 18th ACM Conf. Computer and Comm. Security (CCS '11), pp. 389-400, 2011.

[14] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, "Blueprint for the Intercloud—Protocols and Formats for Cloud Computing Interoperability," Proc. Int'l Conf. Internet and Web Applications and Services, pp. 328-336, 2009.

[15] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "How to Enhance Cloud Architectures to Enable Cross-Federation," Proc. IEEE Third Int'l Conf. Cloud Computing (CLOUD), pp. 337-345, 2010.

[16] R. Turpin and B.A. Coan, "Extending Binary Byzantine Agreement to Multivalued Byzantine Agreement," Information Processing Letters, vol. 18, no. 2, pp. 73-76, 1984.

[17] I. Koren and C.M.C. Krishna, Fault-Tolerant Systems. Morgan Kaufmann, 2007.

[18] J.D.J. Wisner, G.K.G. Leong, and K.-C. Tan, Principles of Supply Chain Management: A Balanced Approach. South-Western, 2011.

[19] N.A.N. Lynch, Distributed Algorithms. Morgan Kaufmann, 1996.

[20] G. Danezis and B. Livshits, "Towards Ensuring Client-Side Computational Integrity (Position Paper)," Proc. ACM Cloud Computing Security Workshop (CCSW '11), pp. 125-130, 2011.

[21] S. Groß and A. Schill, "Towards User Centric Data Governance and Control in the Cloud," Proc. IFIP WG 11.4 Int'l Conf. Open Problems in Network Security (iNetSeC), pp. 132-144, 2011.

[22] R. Rivest, L. Adleman, and M. Dertouzos, "On Data Banks and Privacy Homomorphisms," Foundations of Secure Computation, vol. 4, no. 11, pp. 169-180, 1978.

[23] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[24] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," Proc. 17th Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT '99), pp. 223- 238, 1999.

[25] C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., 2009.

[26] G. Asharov, A. Jain, A. Lo´pez-Alt, E. Tromer, V. Vaikuntanathan, and D. Wichs, "Multiparty Computation with Low Communication, Computation and Interaction via Threshold Fhe," Proc. 31st Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '12), pp. 483-501, 2012.

[27] Y. Desmedt, "Some Recent Research Aspects of Threshold Cryptography," Proc. First Int'l Information Security Workshop, pp. 158-173, 1998.

[28] A.C.A. Yao, "Protocols for Secure Computations," Proc. IEEE 23rd Ann. Symp. Foundations of Computer Science (FOCS '82), pp. 160-164, 1982.

[29] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation," Proc. 20th Ann. ACM Symp. Theory of Computing (STOC '88), pp. 1-10, 1988.

[30] O. Goldreich, S.M.S. Micali, and A. Wigderson, "How to Play Any Mental Game," Proc. 19th Ann. ACM Symp. Theory of Computation (STOC '87), pp. 218-229, 1987.

[31] I. Damga°rd, M. Geisler, M. Krøigaard, and J.B.J. Nielsen,

"Asynchronous Multiparty Computation: Theory and Implementation," Proc. 12th Int'l Conf. Practice and Theory Public Key Cryptography (PKC '09), pp. 160-179, 2009.

[32] M. Burkhart, M. Strasser, D. Many, and X. Dimitropoulos, "SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics," Proc. USENIX Security Symp., pp. 223-240, 2010.

[33] S. Bugiel, S. Nu¨ rnberger, A.-R. Sadeghi, and T. Schneider, "Twin Clouds: Secure Cloud Computing with Low Latency," Proc. 12th IFIP TC 6/TC 11 Int'l Conf. Comm. and Multimedia Security (CMS'11), pp. 32-44, 2011.

[34] P. Bogetoft, D.L.D. Christensen, I. Damgard, M. Geisler, T.P.T. Jakobsen, M. Kroigaard, J.D.J. Nielsen, J.B.J. Nielsen, K. Nielsen, J. Pagter, M.I.M. Schwartzbach, and T. Toft, "Secure Multiparty Computation Goes Live," Financial Cryptography and Data Security, R. Dingledine and P. Golle, eds., pp. 325-343, Springer-Verlag, 2009.

[35] "DEMONS Deliverable D2.4: Preliminary Implementation of the Privacy Preservation Techniques," Giuseppe Bianchi, eds., et al., DEMONS Deliverable D2.4, 2011.

[36] J.-M. Bohli, W. Li, and J. Seedorf, "Assisting Server for Secure Multi-Party Computation," Proc. Sixth IFIP WG 11.2 Int'l Conf. Information Security Theory and Practice: Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems (WISTP '12), pp. 144-159, 2012.

[37] O. Catrina and F. Kerschbaum, "Fostering the Uptake of Secure Multiparty Computation in E-Commerce," Proc. IEEE Third Int'l Conf. Availability, Reliability and Security (ARES '08), pp. 693-700, 2008.

[38] F. Pagano and D. Pagano, "Using In-Memory Encrypted Databases on the Cloud," Proc. First Int'l Workshop Securing Services on the Cloud (IWSSC), pp. 30-37, 2011.

[39] J. Somorovsky, C. Meyer, T. Tran, M. Sbeiti, J. Schwenk, and C. Wietfeld, "SeC2: Secure Mobile Solution for Distributed Public Cloud Storages," Proc. Second Int'l Conf. Cloud Computing and Services Science (CLOSER), pp. 555-561, 2012.

[40] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.

[41] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," Proc. 13th ACM Conf. Computer and Comm. Security, pp. 79-88, 2006.

[42] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions," Proc. 25th Ann. Int'l Conf. Advances in Cryptology (CRYPTO '05), pp. 205-222, 2005.

[43] R. Popa, C. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: Protecting Confidentiality with Encrypted Query Processing," Proc. 23rd ACM Symp. Operating Systems Principles, pp. 85-100, 2011.

[44] A. Boldyreva, N. Chenette, Y. Lee, and A. Oneill, "Order-Preserving Symmetric Encryption," Proc. 28th Ann. Int'l Conf. Advances in Cryptology: The Theory and Applications of Cryptology (EUROCRYPT '09), pp. 224-241, 2009.

[45] J. Vijayan, "Vendors Tap into Cloud Security Concerns with New Encryption Tools," http://www.cio.com.au/article/ 376252/vendors_tap_into_cloud_security_concerns_new_ encryption_tools/, 2013.

[46] L. Wiese, "Horizontal Fragmentation for Data Outsourcing with Formula-Based Confidentiality Constraints," Proc. Fifth Int'l Workshop Security (IWSEC '10), pp. 101-116, 2010.

[47] H. Rajasekaran, L. Lo Iacono, P. Hasselmeyer, J. Fingberg, P. Summers, S. Benkner, G. Engelbrecht, A. Arbona, A. Chiarini, C.M.C. Friedrich, M. Hofmann-Apitius, K. Kumpf, B. Moore, P. Bijlenga, J. Iavindrasana, H. Mueller, R.D.R. Hose, R. Dunlop, and Frangi, "@neurist—Towards a System Architecture forAdvanced Disease Management through Integration of Heterogeneous Data, Computing, and Complex Processing Services,"Proc. IEEE 21st Int'l Symp. Computer-Based Medical Systems (CBMS '08,) pp. 361-366, 2008.

[48] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation),"http://ec.europa.eu/justice/data-protection/ocument/review2012/com_2012_11_en.pdf, 2012.

[49] US Congress, "U.S. Health Insurance Portability and Accountability Act," 1996.

[50] PCI Security Standards Council, "Payment Card Industry (PCI) Data Security Standard - Requirements and Security Assessment Procedures," https://www.pcisecuritystandards.org/documents/pci_dss_v2. pdf, 2010.

[51] US Congress, "Federal Information Security Management Act," http://csrc.nist.gov/drivers/documents/FISMA-final.pdf, 2002.

[52] US General Services Administration, "Federal Risk and Authorization Management Program," http://www.gsa.gov/portal/category/102371, 2012.

[53] European Union, "Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995 L0046:EN:HTML,1995.

[54] European Commission, "Commission Decision of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries under Directive 95/46/EC of the European Parliament and of the Council," Official J. European Union, vol. L39, pp. 5-18, 2010.

[55] EU Article 29 Working Party, "Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data," Recommendation 1/2007, WP 133, http:// ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm, 2007.

[56] Fed. Republic of Germany, "German Federal Data Protection Act (BDSG)," Fed. Law Gazette I, p. 66, 2009.

[57] EU Article 29 Working Party, "Cloud Computing,"Opinion05/2012,WP196, http://ec.europa.eu/justice/data-protection/