THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Ensuring Security at Data Level in Cloud using Multi Cloud Architecture

B. Bhavani Bai
Student of MCA, Santhiram Engineering College, Kurnool, India
N. Rama Devi
HOD of MCA, Santhiram Engineering College, Kurnool, India

Abstract:
The Cloud Computing offers service over internet with dynamically scalable resources. Cloud Computing services provides benefits to the users in terms of cost and ease of use. Cloud Computing services need to address the security during the transmission of sensitive data and critical applications to shared and public cloud environments. The cloud environments are scaling large for data processing and storage needs. Cloud computing environment have various advantages as well as disadvantages on the data security of service consumers. The security issues at various levels of cloud computing environment is identified in this paper and categorized based on cloud computing architecture. This paper focuses on proposing multicloud architecture for ensuring security at data level.

Keywords: *Cloud, Security, Privacy, Multi cloud, Cryptography*

1. Introduction

CLOUD computing offers dynamically scalable resources provisioned as a service over the Internet. The third-party, on-demand, self-service, pay-per-use, and seamlessly scalable computing resources and services offered by the cloud paradigm promise to reduce capital as well as operational expenditures for hardware and software. Clouds can be categorized taking the physical location from the viewpoint of the user into account [1]. A public cloud is offered by third-party service providers and involves resources outside the user's premises. In case the cloud system is installed on the user's premise-usually in the own data center-this setup is called private cloud.

A hybrid approach is denoted as hybrid cloud. This paper will concentrate on public clouds, because these services demand for the highest security requirements but also-as this paper will start arguing-includes high potential for security prospects.

In public clouds, all of the three common cloud service layers (IaaS, Paas, SaaS) share the commonality that the end-users' digital assets are taken from an intraorganiza-tional to an interorganizational context. This creates a number of issues, among which security aspects are regarded as the most critical factors when considering cloud computing adoption [2]. Legislation and compliance frameworks raise further challenges on the outsourcing of data, applications, and processes. One idea on reducing the risk for data and applications in a public cloud is the simultaneous usage of multiple clouds. Several approaches employing this paradigm have been proposed recently. They differ in partitioning and distribution patterns, technologies, cryptographic methods, and targeted scenarios as well as security levels. This paper is an extension of [4] and contains a survey on these different security by multicloud adoption approaches. It provides four distinct models in form of abstracted multi-cloud architectures. These developed multicloud architec-tures allow to categorize the available schemes and to analyze them according to their security benefits. An assessment of the different methods with regards to legal aspects and compliance implications is given in particular.

2. Cloud Security Issues

Cloud computing creates a large number of security issues and challenges. A list of security threats to cloud computing is presented in [5]. These issues range from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. The main problem that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as business-critical data and processes. When considering using a cloud service, the user must be aware of the fact that all data given to the cloud provider leave the own control and protection sphere. Even more, if deploying data-processing applications to the cloud (via IaaS or PaaS), a cloud provider gains full control on these processes. Hence, a strong trust relationship between the cloud provider and the cloud user is considered a general prerequisite in cloud computing. As can be seen from this review of the related work on cloud system attacks, the cloud computing paradigm contains an implicit threat of working in a compromised cloud system. If an attacker is able to infiltrate the cloud system itself, all data and all processes of all users operating on that cloud system may become subject to malicious actions in an avalanche manner. Hence, the cloud computing paradigm requires an in-depth reconsideration on what security requirements might be affected by such an exploita-tion incident. For the common case of a single cloud provider hosting and processing all of its user's data, an intrusion

would immediately affect all security requirements: Acces-sibility, integrity, and confidentiality of data and processes may become violated, and further malicious actions may be performed on behalf of the cloud user's identity.
These cloud security issues and challenges triggered a lot of research activities, resulting in a quantity of proposals targeting the various cloud security threats. Alongside with these security issues, the cloud paradigm comes with a new set of unique features that open the path toward novel security approaches, techniques, and architectures. One promising concept makes use of multiple distinct clouds simultaneously.

3. Multicloud Architectures: Related Work
The basic underlying idea is to use multiple distinct clouds at the same time to mitigate the risks of malicious data manipulation, disclosure, and process tampering. By integrating distinct clouds, the trust assumption can be lowered to an assumption of noncollaborating cloud service providers. Further, this setting makes it much harder for an external attacker to retrieve or tamper hosted data or applications of a specific cloud user. The idea of making use of multiple clouds has been proposed by Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member, IEEE, Luigi Lo Iacono, and Ninja Marnau.
It proposes the following four architectural patterns:

- **Replication of applications** allows to receive multiple results from one operation performed in distinct clouds and to compare them within the own premise (see Section 4). This enables the user to get an evidence on the integrity of the result.

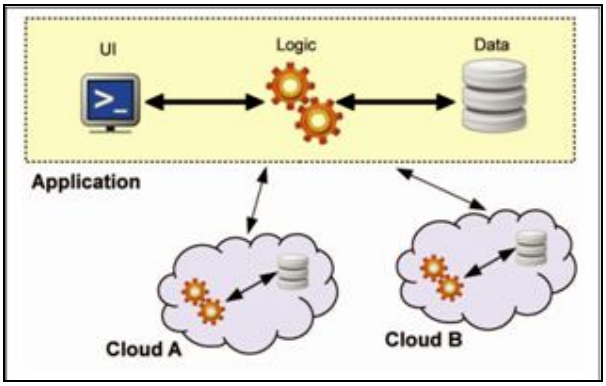

Figure 1: Replication of application systems

- **Partition of application System** into tiers allows to separate the logic from the data (see Section 5). This gives additional protection against data leakage due to flaws in the application logic.

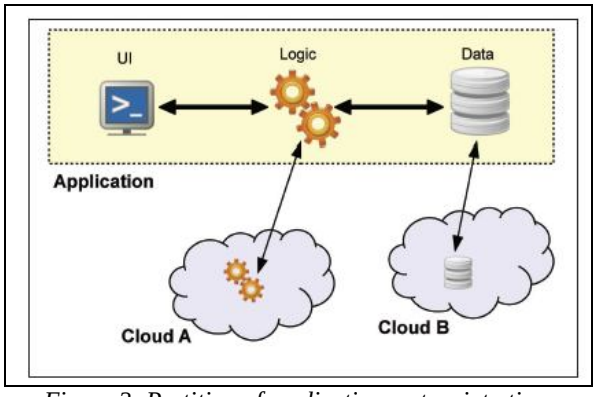

Figure 2: Partition of application system into tiers

- **Partition of application logic into fragments** allows distributing the application logic to distinct clouds. This has two benefits. First, no cloud provider learns the complete application logic. Second, no cloud provider learns the overall calculated result of the application. Thus, this leads to data and application confidentiality.

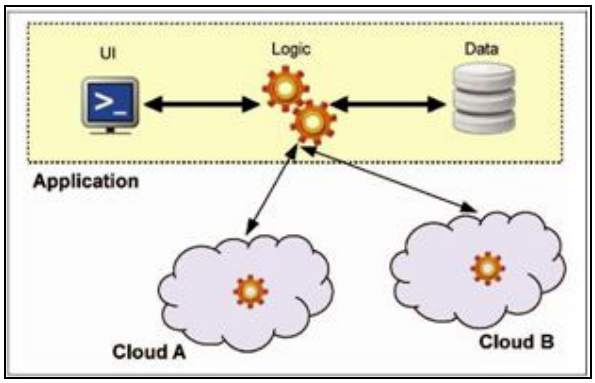

Figure 3: Partition of application logic into fragments

- **Partition of application data into fragments** allows distributing fine-grained fragments of the data to distinct clouds (see Section 7). None of the involved cloud providers gains access to all the data, which safeguards the data's confidentiality.

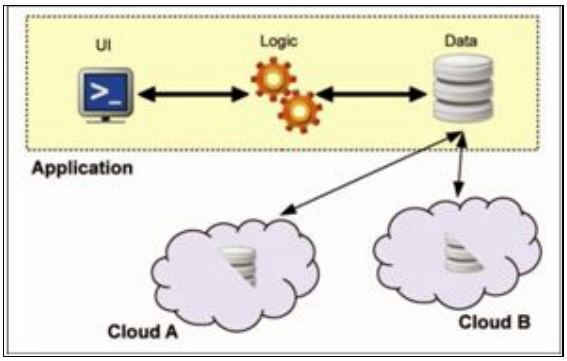

Figure 4: Partition of application data into fragments.

4. Ensuring Security At Data Level In Multi Cloud Architectures

This multi cloud architecture specifies that the application data is partitioned and distributed to distinct clouds (see Fig. 4). The most common forms of data storage are files and databases. Files typically contain unstructured data (e.g., pictures, text documents) and do not allow for easily splitting or exchanging parts of the data. This kind of data can only be partitioned using cryptographic methods (see Section 4.1).

4.1. Cryptographic Data Splitting

Probably, the most basic cryptographic method to store data securely is to store the data in encrypted form. While the cryptographic key could remain at the user's premises, to increase flexibility in cloud data processing or to enable multiuser systems it is beneficial to have the key available online when needed.

The first approach to cryptographic cloud storage is a solution for encrypted key/value storage in the cloud while maintaining the ability to easily access the data. One example of a relational database with encrypted data processing is CryptDB. The database consists of a database server that stores the encrypted data and a proxy that holds the keys and provides a standard SQL interface to the user.

4.1.1. Ensuring Data Security with Encryption Algorithm

The encryption algorithm is most commonly used technique to protect data within cloud environment. The data related to a client can be categorized as public data and private data. The public data is sharable among trusted clients that provide an open environment for collaboration. Private data is client's confidential data that must be transferred in encrypted form for security and privacy. According to key characteristics, modern cryptosystem can be classified into symmetric cryptosystem and asymmetric cryptosystem. For a symmetric cryptosystem, the sender and receiver share an encryption key and decryption key. These two keys are the same or easy to deduce each other. The representatives of symmetric cryptosystem are DES (Data Encryption Standard), 3DES, RC5, RC6, Blowfish, Two-Fish and AES (Advanced Encryption Standard. For an asymmetric cryptosystem, the receiver possesses public key and private key. The public key can be published but the private key should be kept secret. The representatives of asymmetric cryptosystem are RSA (Rivest Shamir Adleman) and ECC (Elliptic Curve Cryptosystem).

The evaluation of various symmetric key encryption algorithms, asymmetric key encryption algorithms and Digital Signature algorithms are studied based on previous researches and different resources. The symmetric encryption algorithms studied are AES, DES, 3-DES, IDES, RC5, and Blowfish. There comparative study based on attributes such as key length, block size, cipher text, developed, security, cryptanalysis resistance, possible keys, possible ASCII printable character key is described with the help of table:

Characteristics	AES	Blowfish	RC5	IDES	3-DES	DES
Key Length	128,192 or 256	32-448 (default 128)	MAX 2040	128	112,168	56
Block Size	128,192 or 256	64	32,64 or 128	64	64	64
Cipher Text	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Developed	2000	1993	1994	1992	1998	1977
Security	Considered Secure	Considered Secure	Considered Secure	Proven Inadequate	Considered secure	Proven Inadequate
Cryptanalysis Resistance	Very Strong against differential, truncated differential, linear, interpolation and square attack	Strong against the standard differential and linear cryptanalysis	Vulnerable against differential, truncated differential, linear, interpolation and square attack	Vulnerableto differential and linear cryptanalysis.	Strong against differential, truncated differential, linear, interpolation and square attack	Vulnerableto differential and linear cryptanalysis, Weak substitution table
Possible Keys	$2^{128},2^{192},2^{256}$	2^{448}	$2^{128},2^{192},2^{256}$	2^{128}	2^{56}(all level)	2^{56}
Possible ASCII Printable Character Key	$95^{16},95^{24},95^{32}$	95^{16}	$95^{16},95^{24},95^{32}$	95^{16}	95^{7}(all level)	95^{7}
Speed	Very Fast	Fast	Slow	Slow	Slow	Very slow

Table 1: Comparative study of various symmetric encryption algorithms

It was concluded from the above comparative study, that AES encryption algorithm is faster, more efficient, and superior in terms of time consumption (encryption/decryption) and throughput under the scenario of data transfer. So it would be better to use AES scheme in encryption of data stored at other end and need to decrypt multiple time. The asymmetric encryption algorithms studied are RSA and Elliptic Curve Cryptography. These algorithms are compared based on main attribute key size with various features such as key generation time, signature generation time and signature verification time are calculated and described in a table as follows:

Characteristics	Elliptic Curve Cryptography	RSA
Key Size (Bits)	163	1024
Key Generation Time (s)	0.08	0.16
Signature Generation (s)	0.15	0.01
Signature Verification (s)	0.23	0.01

Table 2: Comparative study of asymmetric encryption algorithms

It was difficult to state which of asymmetric encryption algorithm is better because RSA performs better when there is no need to generate RSA keys for each use, but rather have fixed RSA keys. With RSA, signature generation and signature verification time is also much less than ECC. But ECC scores over RSA because of less key generation time. ECC is better option when lot of users connects to cloud based services with small session time like cloud based storage. That's why we have used ECC as asymmetric encryption algorithm for our cloud environment. To achieve authentication and non-repudiation purpose within cloud computing environment digital signature has assumed great significance. There are various digital signature algorithms which involves the generation of message digest (hash). MD5 and SHA-1 are well known digital signature generation algorithms and comparative study of these are described with the help of table:

Characteristics	MD5(Message Digest 5)	SHA-512
Message Digest Length	128	512
Attack (For Original message from message digest)	2^{128}	2^{512}
Attack (Find two message for same message digest)	2^{64}	2^{256}
Successful Attack	Some attempt reported	No such claim
Speed	Faster	Slow
Software Implementation	Very easy	Easy

Table 3: Comparative study of digital signature algorithm

The study shows that MD5 is much faster than SHA-512 digital signature algorithm, but with respect to security concerns SHA-512 is more secure than MD5 and no claim of successful attacks with optimal time complexity on SHA-512 has been done so far. The study of various cryptography (Symmetric/Asymmetric) encryption and digital signature algorithms helps to choose the best one from each category to be used in proposed cryptographic module. The symmetric and asymmetric encryption algorithms to be used are AES and ECC respectively. The SHA-512 digital signature generation algorithm is used in combination with ECC asymmetric key encryption algorithm. These algorithms are described as follows: **AES (Advanced Encryption Standard):** The basic steps in algorithm [4] are stated as:

- Key Expansion - round keys are derived from the cipher key using Rijndael's key schedule
- Initial Round AddRoundKey - each byte of the state is combined with the roundkey using bitwise xor

- Rounds-
  SubBytes - a non-linear substitution step where each byte is replaced with another according to a lookup table.
  ShiftRows - a transposition step where each row of the state is shifted cyclicallya certain number of steps.
  MixColumns - a mixing operation which operates on the columns of the state, combining the four bytes in each column.
  AddRoundKey
- Final Round (no MixColumns)- 1. SubBytes 2. ShiftRows 3. AddRoundKey
- Key generation- This module handles key generation by the cryptographic module at client side. The server generates unique keys for users once they authenticate themselves with the server. The key is generated using instances of AES key generator class. This key is then transferred to the cloud client via the mail-server through a mail which receives and stores a copy for it for decrypting purpose.

Elliptic Curve Cryptography (ECC) with SHA-512: An elliptic curve is given by an equation in the form of

$$y^2=x^2+ax+b \quad \text{where } 4a^3+27b^2\neq 0$$

The finite fields those are commonly used over primes (FP) and binary field (F2n). The security of ECC is based on the elliptic curve discrete logarithm problem (ECDCP). This problem is defined as: Given point X, Y on elliptic curve, find z such that X=zY. The following steps describe how ECC works with SHA-512. ECC key generation**:** To generate a public and private key pair for use in ECC communication the steps followed are:

- Find an elliptic curve E(K), where K is a finite field such as Fp or F2n, and a find point Q on E(K). n is the order of Q.
- Select a pseudo random number x such that $1 \leq x \leq (n - 1)$.
- Compute point P = xQ.
- ECC key pair is (P, x), where P is public key, and x is private key.

Signature Generation: To create a signature S for message m, using ECC key pair (P, K) over E(k), the following steps followed:

- Generate a random number k such that $1 \leq k \leq (n - 1)$.
- Compute point kQ = (x1, y1).
- Compute r = x1 (mod n). If r = 0, go to step 1.
- Compute k-1 (mod n).
- Compute SHA-512(m), and convert this to an integer e.
- Compute s = k-1(e + xr) (mod n). If s = 0, go to step 1.
- The signature for message m is S = (r, s).

Signature Verification: This part verify a signature s=(r,s) for message m over a curve E(k) using the public key P performing steps:

- Verify r and s are integers over the interval [1, n - 1].
- Compute SHA-512(m) and convert this to an integer e.
- Compute w = s-1(mod n).
- Compute u1 = ew (mod n) and u2 = rw (mod n).
- Compute X = u1Q + u2P
- If X = 0, reject S. Otherwise, compute v = x1 (mod n).
- Accept if and only if v = r.

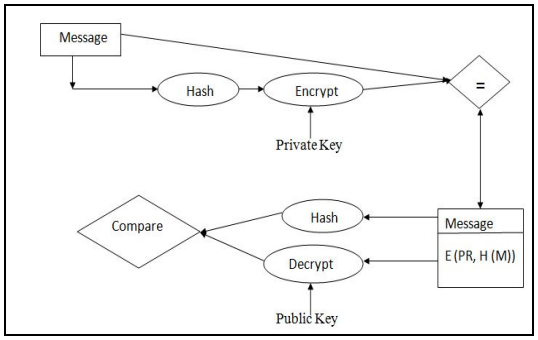

Figure 5: Basic operation of Asymmetric Key encryption Algorithm with Digital Signature

Samba Server: It is a Data Server is used to provide uploading and downloading of files to the users.

The evaluation of various symmetric key encryption algorithms, asymmetric key encryption algorithms and Digital Signature algorithms are studied based on previous researches and different resources. The symmetric encryption algorithms studied are AES, DES, 3-DES, IDES, RC5, and Blowfish. There comparative study based on attributes such as key length, block size, cipher text, developed, security, cryptanalysis resistance, possible keys, possible ASCII printable character key is described with the help of table:

Cloud architecture is designed by combining cryptographic algorithms with samba storage environment. The cryptographic algorithms to be used are selected based on comparative study from previous researches. So the symmetric, asymmetric and digital signature algorithms selected are AES, ECC and SHA respectively to be used for cryptographic application.
The cryptographic application is used to encrypt and decrypt data, provides options to application user whether to use asymmetric with digital signature or symmetric algorithm. Samba server supports owner, group and global attributes associated with files/directories having possible values read, write and execute. Application users will decide whether to use AES algorithm, ECC with digital signature algorithm or disable encryption based on confidentiality, integrity and authentication level required on data which is to be stored on samba storage. The users are guided to select ECC with digital signature option for high level of confidentiality, authentication and integrity with data.
There must be some data that needs high availability among some users defined under a specific group. Another option with AES encryption algorithm supports user to encrypt data and define the group whose users can decrypt and use this data. The disable option provided with cryptographic application disable all options for user and supports upload/download functions without any cryptographic operation. The security mechanism adopted for cloud architecture based on confidentiality, integrity and authenticity of stored data is a two level authentication mechanism.

- Username and password based authentication mechanism: User is asked for a valid username and password provided at the time when samba clients are added with storage environment. The username and password are stored on samba storage verified and validated for every user logging storage area.
- Key based authentication mechanism: This mechanism is supported with the help of mail server. While using cryptographic application for data encryption and decryption data secret key is generated for encryption using AES symmetric key encryption algorithm and same key is used for decryption of encrypted data. The data encrypted with symmetric algorithm is available for group users, so secret key is transferred to each group user through a mail server configured for each user. For data encrypted with asymmetric algorithm public key is transferred to user's mail server inbox for decryption process. The keys are stored within user's mail storage space.

4.2. Proposed Cloud Architecture

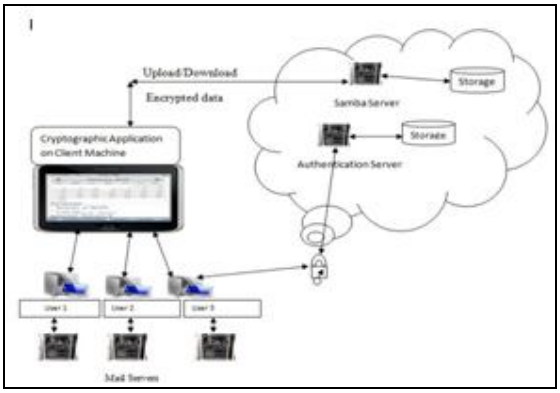

Figure 6

Proposed Cloud architecture is enhanced security model for data storage within cloud environment. It consists of various users with local availability of mail server and cryptographic application. A cryptographic application installed on client side will connect user with samba storage and allows for encryption and decryption operation on data. As the cryptographic application is installed on client's machine it will increase speed-up ratio and mean processing [5] for encryption and decryption process. The authentication server used for authenticating users to enter into server environment and use available functionalities. The various steps followed are explained in terms of communication among Client machine provided with cryptographic module and samba server storage.

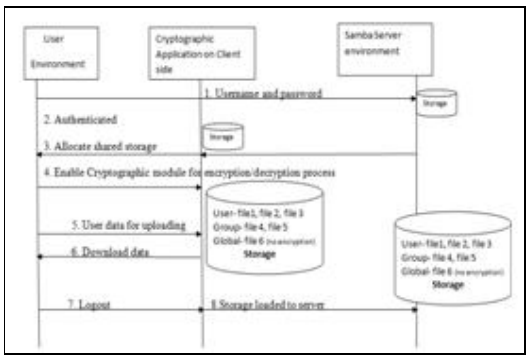

Figure 7: Sequence diagram for describing interaction among samba server and user

Step 1: Username and password allocated to user for access to samba server storage. Step 2: Verification and validation are performed by matching details stored in samba server storage. Step 3: After user authentication storage is allocated to user for uploading and downloading. Step 4: Cryptographic application based on AES and ECC with SHA used for encryption/decryption operation on data. Step 5: The user provided with storage space decide to upload data using encryption application or directly on samba storage. Step 6: Data downloaded from storage space and decrypted using key stored in user's mail server. Step 7: After upload and download user logout from server storage. Step 8: Storage loaded to server and connection terminated.

5. Legal Compliance With Multicloud Architectures

Since legislation traditionally only slowly copes with technological paradigm shifts, there are few to none cloud specific regulations in place by now. Therefore, for cloud computing the same legal framework is applicable as for any other means of data processing. Generally, legal compliance does not distinguish between different means of technology but rather different types of information. For instance, enterprises are facing other legal requirements for the lawful processing of their tax information than for the lawful processing of their Customer Relationship Manage-ment. A one-cloud-fits-all approach does not reflect these differing compliance requirements.

5.1. Partition of Application Logic/Data

5.1.1. Obfuscating Splitting and Database Splitting

These approaches are especially valuable for dealing with personal identifiable data. Segmenting personal identifi-able data—if realized in a reasonable way—is a viable privacy safeguard. Best practice would be to separate the data in a way that renders the remaining data pseudon-ymous. Pseudonymity itself is a privacy safeguard (see [56, Section 3a]). Therefore, outsourcing pseudonymized in-formation, which is unlinkable to a specific person, does require considerable less additional safeguards as com-pared to nonpseudonymized information.

Pseudonymization based on the Obfuscated Splitting approach could be used, e.g., in Human Resources or Customer Relationship Management. A potential cloud customer would have to remove all directly identifying data in the first place, like name, social security number, credit card information, or address, and store this information separately, either on premise or in a cloud with adequately high-security controls. The remaining data can still be linked to the directly identifying data by means of an unobvious identifier (the pseudonym), which is unusable for any malicious third parties. The unlinkability of the combined pseudonymized data to a person can be ensured by performing a carefully conducted privacy risk assess-ment. These assessments are always constrained by the assumptions of an adversary's "reasonable means" [53, Recital 26]. The cloud customer has the option to outsource the pseudonymized data to a cloud service provider with fewer security controls, which may result in additional cost savings. If the customer decides to outsource the directly identifiable data to a different cloud service provider, she has to ensure that these two providers do not cooperate, e.g., by using the same IaaS provider in the backend.

5.1.2. Cryptographic Data Splitting and Homomorphic Encryption

As of today, this approach appears to be the most viable alternative, both from the technical and economical point of view. State-of-the-art encryption of data with adequate key management is one of the most effective means to safeguard privacy and confidentiality when outsourcing data to a cloud service provider. Nevertheless, at least in the European Union, encryption is not considered to relieve cloud customers from all of their responsibilities and legal obligations. Encrypted data keep the nature it has in its decrypted state; personally identifiable information in encrypted form is still regarded as personally identifiable information. Encryption is considered as an important technical security measure; however, some additional mandatory legal safeguards still apply. For personally identifiable data, this means that, e.g., adequate contracts for the export of data to countries outside of the European Economic Area have to be in place.

6. Assessment of Multicloud Architectures

The compliance dimension provides a high-level indica-tion of the impact of each approach to the legal obligations implied to the cloud customer when utilizing that approach. Application of the dual execution approach, for instance, may be favorable in terms of security and feasibility, but requires complex contractual negotiations between the cloud custo-mer and two different cloud providers, doubling the workload and legal obligations for the whole cloud application. Equivalently, the use of more than two different cloud providers (n clouds approach) improves on integrity and availability, but also requires n contract negotiations and risk assessments, amplified by the necessity to assess the risks associated with automated detection and correction of irregularities within the n parallel executions.

7. Conclusion

The use of multiple cloud providers for gaining security and privacy benefits is nontrivial. As the approaches investigated in this paper clearly show, there is no single optimal approach to foster both security and legal com-pliance in an omniapplicable manner. Moreover, the approaches that are favorable from a technical perspective appear less appealing from a regulatory point of view, and vice versa. The few approaches that score sufficiently in both these dimensions lack versatility and ease of use, hence can be used in very rare circumstances only.

As can be seen from the discussions of the four major multicloud approaches, each of them has its pitfalls and weak spots, either in terms of security guarantees, in terms of compliance to legal obligations, or in terms of feasibility. Given that every type of multicloud approach falls into one of these four categories, this implies a state of the art that is somewhat dissatisfying.

However, two major indications for improvement can be taken from the examinations performed in this paper. 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 combining the approaches presented here. For instance, using the n clouds approach (and its integrity guarantees) in combination with sound data encryption (and its confidentiality guarantees) may result in approaches that suffice for both technical and regulatory requirements. We explicitly do not investi-gate this field here—due to space restrictions; however, we encourage the research community to explore these combinations, and assess their capabilities in terms of the given evaluation dimensions.

Second, we identified the fields of homomorphic en-cryption and secure multiparty computation protocols to be highly promising in terms of both technical security and regulatory compliance. As of now, the limitations of these approaches only stem from their narrow applicability and high complexity in use. However, given their excellent properties in terms of security and compliance in multi-cloud architectures, we envision these fields to become the major building blocks for future generations of the multi-cloud computing paradigm.

8. 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 Comput-ing 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-without-permission/, 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. 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.
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 Agree-ment to Multivalued Byzantine Agreement," Information Proces-sing 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 Communica-tion, Computation and Interaction via Threshold Fhe,” Proc. 31st Ann. Int’l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT ’12), pp. 483-501, 2012. Y. Desmedt, “Some Recent Research Aspects of Threshold Cryptography,” Proc. First Int’l Information Security Workshop, 158-173, 1998.
27. A.C.A. Yao, “Protocols for Secure Computations,” Proc. IEEE 23rd Ann. Symp. Foundations of Computer Science (FOCS ’82), pp. 160-164, 1982.
28. 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.
29. 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.
30. I. Damga˚rd, M. Geisler, M. Krøigaard, and J.B.J. Nielsen, “Asynchronous Multiparty Computation: Theory and Implemen-tation,” Proc. 12th Int’l Conf. Practice and Theory Public Key Cryptography (PKC ’09), pp. 160-179, 2009.
31. 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.
32. 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.
33. 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.
34. “DEMONS Deliverable D2.4: Preliminary Implementation of the Privacy Preservation Techniques,” Giuseppe Bianchi, eds., et al., DEMONS Deliverable D2.4, 2011.
35. 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.
36. 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), 693-700, 2008.
37. F. Pagano and D. Pagano, “Using In-Memory Encrypted Data-bases on the Cloud,” Proc. First Int’l Workshop Securing Services on the Cloud (IWSSC), pp. 30-37, 2011. J. Somorovsky, C. Meyer, T. Tran, M. Sbeiti, J. Schwenk, and 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.
38. S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. 14th Int’l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.
39. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable Symmetric Encryption: Improved Definitions and Efficient Con-structions,” Proc. 13th ACM Conf. Computer and Comm. Security, pp. 79-88, 2006. M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, Malone-Lee, G. Neven, P. Paillier, and H. Shi, “Searchable Encryption Revisited: Consistency Properties, Relation to Anon-ymous IBE, and Extensions,” Proc. 25th Ann. Int’l Conf. Advances in Cryptology (CRYPTO ’05), pp. 205-222, 2005.
40. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable Symmetric Encryption: Improved Definitions and Efficient Con-structions,” Proc. 13th ACM Conf. Computer and Comm. Security, pp. 79-88, 2006.
41. M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, Malone-Lee, G. Neven, P. Paillier, and H. Shi, “Searchable Encryption Revisited: Consistency Properties, Relation to Anon-ymous IBE, and Extensions,” Proc. 25th Ann. Int’l Conf. Advances in Cryptology (CRYPTO ’05), pp. 205-222, 2005.
42. 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.
43. 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.
44. 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.
45. L. Wiese, “Horizontal Fragmentation for Data Outsourcing with Formula-Based Confidentiality Constraints,” Proc. Fifth Int’l Work-shop Security (IWSEC ’10), pp. 101-116, 2010. 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 for Advanced Disease Management through Integration of Hetero-geneous Data, Computing, and Complex Processing Services,” Proc. IEEE 21st Int’l Symp. Computer-Based Medical Systems (CBMS ’08,) pp. 361-366, 2008.
46. 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/ document/review2012/com_2012_11_en.pdf, 2012.
47. US Congress, “U.S. Health Insurance Portability and Account-ability Act,” 1996.
48. PCI Security Standards Council, “Payment Card Industry (PCI) Data Security Standard - Requirements and Security Assess-ment Procedures,” https://www.pcisecuritystandards.org/ documents/pci_dss_v2.pdf, 2010.
49. US Congress, “Federal Information Security Management Act,” http://csrc.nist.gov/drivers/documents/FISMA-final.pdf, 2002.

50. US General Services Administration, "Federal Risk and Author-ization Management Program," http://www.gsa.gov/portal/ category/102371, 2012.
51. 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:31995L0046:EN:HTML, 1995.
52. 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.
53. 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.
54. Fed. Republic of Germany, "German Federal Data Protection Act (BDSG)," Fed. Law Gazette I, p. 66, 2009.
55. EU Article 29 Working Party, "Cloud Computing," Opinion 05/ 2012, WP 196, http://ec.europa.eu/justice/data-protection/ article-29/documentation/opinion-recommendation/files/2012/ wp196_en.pdf, 2012.
56. EU Article 29 Working Party, "Cloud Computing," Opinion 05/ 2012, WP 196, http://ec.europa.eu/justice/data-protection/ article-29/documentation/opinion-recommendation/files/2012/ wp196_en.pdf, 2012.
57. "Security and Privacy Enhancing Multicloud Architectures", Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member, IEEE,Luigi Lo Iacono, and Ninja Marnau