International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 08 | August - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

An Effective Security Mechanism for Users Data in Cloud Computing with Security Certification System

Gumma Parvathi Devi[1]
Assistant Professor, Department of CSE(AIML), CMR Technical Campus, Hyderabad .

Abstract: Data integrity is the reliability of the data, whereas cloud computing security is the protection of the data. Data security and integrity are two different concepts. As a result, they are both crucial in the field of cloud computing. The security and integrity of data are a top issue for users in relation to cloud computing. This essay's goal is to examine the risks and remedies related to the issues users of cloud computing must deal with regarding data security and data integrity. While data reliability is concerned with data accuracy, data protection is concerned with data security. A data security policy aims to lower the possibility of emails, medical records, corporate papers, and trade secrets leaking. In information technology, data integrity, security, and privacy are crucial. Data consistency, correctness, and reliability, on the other hand, ensure that digital data is not tampered with and that only authorised users may access or alter the data. Users can trust a number of sites since they utilise more understandable language to make their terms more transparent. The foundation of cloud computing is sharing computer resources among many users. A number of policies are created to guarantee legal compliance while safeguarding the data, programmes, and infrastructure related to cloud computing. We provide a test-based assurance scheme intended for grading security. Our plan evaluates how current certification procedures will be affected by changes to the cloud, systems, and methodology levels of certification. The suggested strategy reduces the likelihood of needless certificate revocation and, to the greatest extent possible, the volume of re-certification activities. To accomplish this, it re-validates existing certificates when pertinent changes are noticed by using the evidence that is already present in them.

Keywords: Cloud computing, security certification system, data security, distributed access.

1.INTRODUCTION

A new computer architecture called cloud computing connects massive computing resources for effective integration and provides consumers with computing resources as a service. Users don't need to take into account the difficulties of the underlying implementation and management in order to access virtual computers and storage systems on demand through the broadband network, significantly lowering the difficulty and hardware required to realise the user's investment.

With cloud computing, physical and virtual services are actually separated, corporate services are more affordable, and network resources are used more efficiently [1]. With the advancement of cloud computing applications and research both domestically and internationally, the field's development must contend with a number of pressing problems. Security concerns dominate this list, and as cloud computing gains popularity, their significance has been reduced. According to a 2009 Gartner poll, 70% of participants think that the current cloud computing CTO's lack of use of the main justifications is due to worries about data security and privacy. Recent security incidents sponsored by Amazon, Google, and other cloud computing providers have heightened people's concerns. For instance, in March 2009, Google allowed a large amount of user files to leak; in February 2009 and July, Amazon's "Simple Storage Service" (also known as S3), which depends on two breaks, caused its website to come to a complete stop; etc. Therefore, we must thoroughly analyse and address the cloud computing security vulnerabilities that are now present in order to ensure that companies and organisations who use cloud computing platforms on a broad scale can safely deliver their own data management to the cloud service provider [3].

A new IT vision in which software and computational resources are made available as services across a virtualized ICT infrastructure that is accessed over the Internet is supported by the cloud computing paradigm. The flexibility and lower costs of owning, running, and maintaining the computational infrastructures that cloud computing offers come at the cost of more security risks and worries. In reality, users that deploy a service in the cloud cede full ownership of their data and apps to cloud providers, who may hold them entirely or in part.

To boost user trust and confidence in ICT systems, assurance approaches including audit, certification, and compliance [2] have been defined. Security assurance techniques must offer reliable proof that cloud-based

systems will function as intended and that cloud providers will handle and use users' data and apps in accordance with their rules and wishes.

In this study, we concentrate on cloud certification, which has recently been suggested as a potential technique for cloud assurance [2] and [5]. By using testing and/or monitoring by a reputable third party, cloud certification schemes seek to provide certified proof of a certain cloud-based system's non-functional characteristics.

To manage evolutionary scenarios where cloud events, ongoing system improvements, and modifications to the certification methodology would necessitate an adaptation of the certification process, cloud certification is now required.

The majority of current systems do not accommodate evolutionary scenarios and necessitate re-certification from scratch, whose high costs are likely to negate the benefits provided by certification procedures. Few strategies for supporting incremental certification of developing systems have only lately been proposed. These methods primarily address situations in which certification adaptation is carried out manually and imposes a significant burden on developers and certification authorities [7], is brought about only by modifications to the certified service [8] or is carried out on purpose [9]. In a cloud environment, we prefer to enable an incremental certification strategy that is semi-automatic and handles runtime cloud events, infrastructure changes, and methodology modifications.

A test-based incremental security certification programme is described in this paper's methodology for cloud-based systems.

Our plan adapts current certification procedures and certificates to runtime modifications to the cloud, the system being certified, and the methodology for certification.

In order to achieve the dynamics of cloud environments, it i) minimises the number of testing activities that must be performed on certified systems; ii) reuses evidence created as part of a prior certification process and adapts it to pertinent changes; and iii) works at all layers of the cloud stack.

II.RELATED WORKS

Several websites have been reviewed in order to comprehend the fundamentals of cloud computing and keeping data securely on the cloud. This part offers a survey of the literature to lay the groundwork for talking about various data security issues.

Moiz, Venkata, and Srinivas offer a clear understanding of cloud computing's fundamental ideas. By giving examples of applications that can be created utilising cloud computing and how they can assist the developing world in utilising this growing technology, several fundamental themes are covered in this study [1].

On the other side, Chen and Zhao have talked about the consumers' worries about transferring their data to the cloud.

Chen and Zhao claim that security concerns are one of the main barriers keeping big businesses from moving their data to the cloud. The authors' analysis of concerns relating to cloud data security and privacy protection is excellent.

They have also talked about some of the options for resolving these problems [5,6]. Hu and A. Klein did, however, offer a standard for cloud data security while it is in transit. To protect data during relocation, a baseline for encryption has been discussed. Robust security necessitates further encryption, but doing so requires additional computing. The benchmark they addressed in their paper exhibits equilibrium for the overhead associated with security and encryption [7].

Tjoa, A.M. and Huemer examine the privacy issue by preserving data control to the end user to surge confidence. Several Cloud computing attacks are reviewed and some solutions are proposed to overcome these attacks [8].

Therefore, Abdelkader and Etriby propose a data security model for cloud computing based on cloud architecture. They also developed software to enrich the effort in Data Security model for cloud computing further [9].

In 2016 Sarojini et.al proposed a technique known as Enhanced Mutual Trusted Access Control Algorithm (EMTACA). This technique presents a mutual trust for both cloud users and cloud service providers to avoid security related issues in cloud computing [10]. The aim of this paper is to propose a system which include EMTACA algorithm which can assure enhanced guaranteed and trusted and reputation based cloud services among the users in a cloud environment [10]. The results of this paper showed data confidentiality, integrity and availability which is the three most important aspect of data security was achieved.

In 2017, Dimitra A. Geogiou wrote a paper to present security policies for cloud computing. The purpose of the security policies is to protect people and information, set rules for expected behavior by users, minimize risks and help to track compliance with regulation [11]. The paper focused on Software as a Service. The paper presented a detailed review and analysis of existing studies as far as security is concern in cloud computing. With Dimitra's review of existing threat, he focused on the once that are not applicable to conventional systems [11]. To be able to identify new rules that supposed to be integrated in the cloud policy, a methodology was proposed for assessing different threats in the cloud. This paper scrutinized the security requirements of a cloud service provider taking into consideration a case study of E-health system of Europe.

III.SECURITY CERTIFICATION SYSTEM

A certification process is a group effort with the goal of demonstrating that a particular system complies with certain specifications and operates as expected [10]. In this paper, we focus on a certification process for cloud-based security that includes a service provider that owns the cloud-based system that needs to be certified, a cloud provider that opens up its infrastructure to support certification activities, a certification authority that oversees the certification process, and a lab that has been accredited and to which the certification authority has delegated responsibility for all evaluation tasks.
To certify its backend services, the cloud provider can function as a service provider, as we note.

The Target of Certification (ToC) system under assessment, the security property p to be certified, and the list of evaluation activities are inputs into the certification process. The result of the certification process is a certificate describing a set of evidence e confirming the support of p by ToC. It consists of the following two primary phases.

1) The certification methodology specification is handled by the certification authority and outlines a series of tasks that must be completed on a class of ToC in order to demonstrate a particular property. A machine-readable document called Certification Model (CM) Template T that has been authorised by the certification authority outlines the certification technique.

2) Implementation of the proposed approach for certification is done jointly by the service provider and the accredited lab on a particular ToC to demonstrate a property p. In order to certify the necessary ToC, a machine-readable document called Certification Model (CM) Instance I is first defined as an instantiation of T.

A security certification system process involves the evaluation and assessment of an organization's or individual's security practices, controls, and processes against established security standards and frameworks. This process aims to determine whether the organization or individual meets the specified security requirements and is capable of effectively managing and mitigating security risks. Here's a general outline of the steps involved in a security certification system process:

Select a Security Standard or Framework: Choose a relevant and widely recognized security standard or framework that aligns with the industry, regulatory requirements, or the specific security goals of the organization. Examples include ISO 27001, NIST SP 800-53, CIS Critical Security Controls, etc.

Preparation and Gap Analysis: Assess the current security practices, controls, and processes of the organization or individual against the chosen security standard. Identify gaps between the existing practices and the requirements of the standard. This step helps create a roadmap for achieving certification.

Security Documentation: Develop or update security policies, procedures, guidelines, and documentation as required by the chosen standard. This documentation provides evidence of the implementation of security controls and practices.

Implementation of Controls: Implement the necessary security controls and practices as outlined by the chosen security standard. This may involve technological, procedural, and organizational changes to enhance security posture.

Security Risk Assessment: Conduct a comprehensive risk assessment to identify potential threats, vulnerabilities, and risks to the organization's assets. This assessment helps in determining appropriate security measures to mitigate these risks.

Internal Audits: Conduct internal audits to assess the organization's readiness for the certification process. These audits help identify any remaining gaps and ensure that the implemented controls are effective.

Remediation: Address any identified gaps, vulnerabilities, or weaknesses in the security practices based on the findings of internal audits and risk assessments.

Third-Party Assessment: Engage a third-party certification body or auditor to perform an independent assessment of the organization's security practices. The auditor evaluates the implementation of controls, documentation, and processes to determine compliance with the chosen standard.

Certification Audit: The third-party auditor conducts a formal certification audit. This audit involves reviewing documentation, interviewing key personnel, and assessing the effectiveness of security controls. The audit can be conducted in stages or as a single comprehensive review.

Audit Report and Decision: The auditor provides a detailed report of findings, including identified strengths, weaknesses, and recommendations. Based on the audit report, the certification body makes a decision regarding whether to grant certification.

Certification and Maintenance: If the organization or individual meets the requirements of the chosen standard, they are awarded the certification. This certification is typically valid for a certain period (e.g., one to three years). The certified entity must undergo regular surveillance audits to maintain the certification status.

Continuous Improvement: Security certifications require ongoing efforts to maintain and improve security practices. Organizations must continuously monitor and assess their security posture, address emerging threats, and adapt to changes in technology and regulations.

It's important to note that the specific steps and details of the certification process may vary depending on the chosen security standard, the industry, and the certification body involved. It's recommended to consult the official documentation of the chosen standard and engage with reputable certification bodies to ensure a thorough and successful certification process.

IV.CLOUD SECURITY

Cloud security refers to the practice of protecting data, applications, and infrastructure in cloud computing environments. Cloud security aims to ensure the confidentiality, integrity, and availability of resources while managing the unique risks associated with cloud services. As organizations increasingly adopt cloud computing, understanding and implementing effective cloud security measures is crucial to prevent data breaches, unauthorized access, and other security incidents. Here are some key aspects and best practices related to cloud security:

Shared Responsibility Model:

Cloud service providers (CSPs) typically follow a shared responsibility model, where the provider is responsible for securing the underlying infrastructure, while customers are responsible for securing their data, applications, and configurations. Understanding this division of responsibilities is fundamental to implementing effective cloud security.

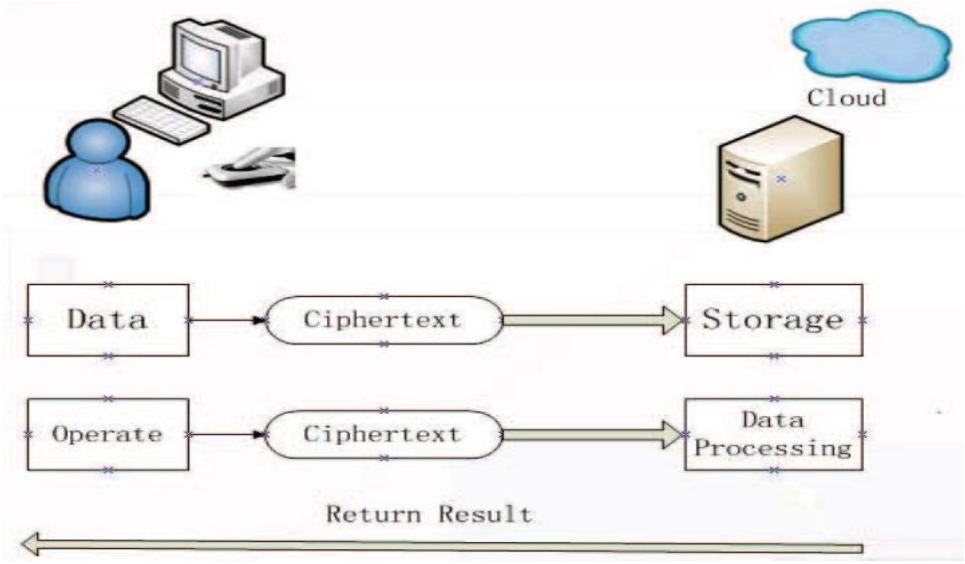

Figure 1. Schematic diagram of cloud computing data security

Identity and Access Management (IAM):

Implement strong identity and access management controls. Use multi-factor authentication (MFA), role-based access control (RBAC), and principle of least privilege to ensure that only authorized users can access resources.

Encryption:

Use encryption to protect data at rest, in transit, and during processing. Encryption prevents unauthorized access even if data is compromised. Cloud providers often offer encryption services and key management solutions.

Network Security:

Secure your network by configuring firewalls, virtual private networks (VPNs), and intrusion detection/prevention systems (IDS/IPS). Use security groups and network access control lists to control traffic to and from your cloud resources.

Patch Management:

Regularly update and patch the operating systems, applications, and software used in your cloud environment to address known vulnerabilities.

Data Protection:

Implement data loss prevention (DLP) measures to prevent sensitive information from being leaked or shared inappropriately. Define and enforce data classification policies.

Security Monitoring and Logging:

Monitor cloud resources for suspicious activities and potential security breaches. Enable logging and use security information and event management (SIEM) tools to analyze and respond to incidents.

Incident Response Plan:

Develop an incident response plan specific to cloud environments. This plan outlines the steps to take in case of a security incident, including who to contact, how to isolate affected resources, and how to recover.

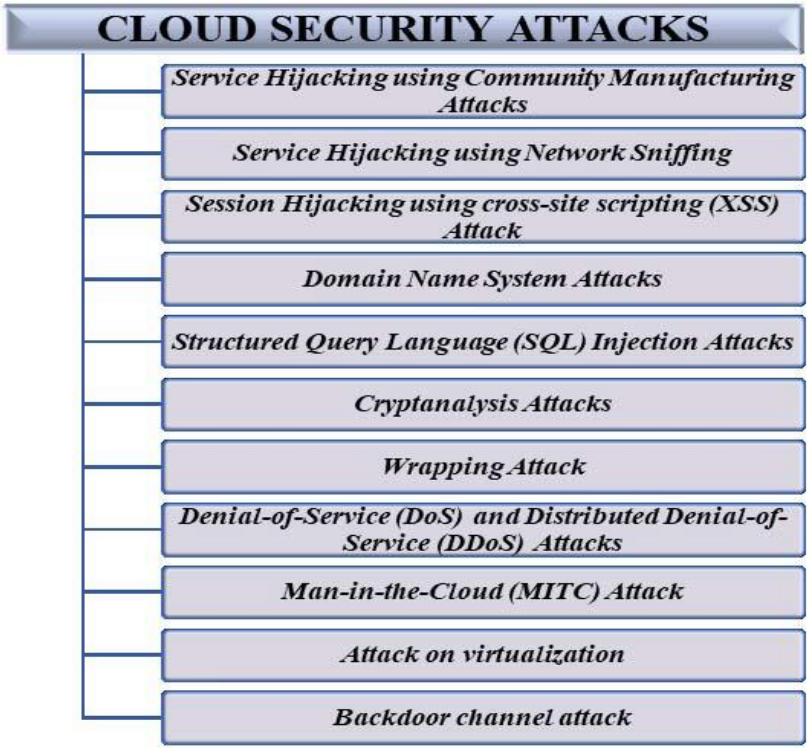

Fig 2. Cloud Security Attacks

Cloud-Specific Threats:

Understand cloud-specific threats such as data leakage due to misconfigurations, insecure APIs, and insider threats. Cloud security posture management (CSPM) tools can help identify and mitigate these risks.

Vendor Assessment and Due Diligence:
Before selecting a cloud service provider, assess their security practices, compliance certifications, and data protection measures. Ensure they meet your organization's security requirements.

Compliance and Regulations:
Ensure that your cloud environment complies with relevant industry regulations and standards, such as GDPR, HIPAA, PCI DSS, etc. Many cloud providers offer compliance documentation and features to help with this.

Employee Training and Awareness:
Educate your employees about cloud security best practices, the risks of cloud computing, and the importance of adhering to security policies.

Regular Audits and Assessments:
Perform regular security audits and assessments to identify vulnerabilities and ensure that security controls are effectively implemented and maintained.

Remember that cloud security is an ongoing process. As technology and threats evolve, your cloud security strategy should adapt accordingly. Stay informed about the latest security trends, engage with your cloud service provider's resources, and continuously improve your cloud security posture.

V. AUDITING AND UNIT TESTING

The auditing and upkeep of cloud services should be under the authority of cloud providers. It can be done by continuously checking the logs of users and the administrative sessions with the user-affected areas of cloud services. The trace-back method is used to track down users who break the rules and the law. The goal of cloud testing is to balance the benefits and dangers of cloud computing services.

Both users and cloud service providers test the cloud to their respective degrees.

The customer, on the other hand, is in charge of conducting tests to eliminate or reduce any risk to its business or clients. In a cloud security paradigm, the cloud services provider protects the physical security of the architecture through controls and auditing mechanisms to thwart cold-boot attacks. The default level of security measures for users must be specified by the cloud service manager. Cloud service managers keep an eye out for malicious attacks from renters that aim to damage the virtual machines of other tenants. Researchers asserted in that cloud vendors' primary concern was the protection of multi-tenancy regions.

Cloud services are well-known methods for industrial systems to provide data integration and sharing services for product traceability. Malicious cloud services, however, impede commercial parties from correctly acquiring product traceability. Acics is suggested by recent study as a reliable and quick auditing schema for the vast industrial data in the unreliable cloud computing environment. With the use of this schema, industry players can act as product consistency auditors.
The proposed Acics is more effective in data consistency verification of small volumes of items at a reasonable cost, according to experimental results when compared to other methodologies. Better read or write latency rates can be seen using the suggested Acics schema.

This schema can be studied in upcoming studies as it has not been tested on large products.Prior to the later study under evaluation, research [29] had shown that cloud computing posed a serious security risk to the data of its users. Customers move their data to the CSP's storage but do not assess the CSP's security measures to safeguard their sensitive data. The Cloud Security Alliance (CSA) establishes the standards for evaluating the security controls within the CSP organisation. It helps a cloud service user to have faith in CSPs' services. The fundamental problem is that the accuracy of the responses to the questionnaire-based security evaluation by CSA is not validated. A framework suggested in the same study uses third party auditors (TPAs) to validate the participants' responses in an effort to close this gap.

However, there is no method for external users to use the results of third party inspection. Users' feedback is necessary to further evaluate the quality of cloud providers' services and increase users' trust in an organization's cloud services.

A serious risk to cloud security is data loss as a result of data leaking. Without preserving the backup copy, data compromises and modifications take place by changing or erasing the original data. Data storage on cloud media is also less dependable because it is accessible to both insiders and outside parties. The corporations' cloud service offerings are viewed as dishonest by irresponsible media [7]. The latter problem can be solved using a utility-based approach by identifying users' harmful behaviour. Users are able to restore their data with this tool. In contrast to other cloud services, the Unity service is a personal repository service.

Users of cloud services do not need to use them without authorization, although CSP organisation employees sometimes act maliciously. We discovered such events in research and, which can jeopardise cloud service providers' data security. Therefore, a unity model emphasises the development of trust between clients and cloud service providers.While customers access cloud computing services over the internet, the new paradigm of cloud computing ensures their dependability, availability, and scalability. In response to user requests, the notion of software and services is activated.

However, the effective organisation has identified a number of new concerns. Since everything is held inside the cloud computing box, a hacker can use methods to steal the confidential information. Hackers can be stopped from gaining unauthorised access to cloud data thanks to advancements in the security disciplines. Additionally, other security measures should be suggested to give users complete data security.It is possible to extend key splitting and homomorphic encryption to make new advancements in this field of study. The focus of was on safe data transfer across encrypted communication routes between clients and cloud computing providers.

In [4], a group of researchers devised an attack model and identified the three most suspect clients.
Researchers detected the dubious customer behaviour using datasets from Google.

VI.CONCLUSION

Rapid system setup, cost savings, enormous storage capacity, and simple system access from anywhere at any time are all advantages of cloud computing. By offering seamless and robust functioning, regardless of the resources, it seeks to empower the user. Therefore, it is clear that cloud computing is a rapidly evolving technology and a widely used computing environment worldwide. In comparison to traditional environments,

cloud computing offers a number of benefits, including the capacity to manage the majority of unexpected spikes in application or service demand. However, there are a number of privacy and security issues that prevent cloud computing from being widely used. All users must be aware of the threats, dangers, and attacks that exist in the cloud.The corporations' quick adoption of the cloud is a result of their understanding of security issues and assaults. Cloud computing also makes use of several established and cutting-edge technology. These developing technologies may lead to a variety of cloud security-related problems. Users from different locations can access the same physical resources in the cloud thanks to virtualization and the multi-tenancy concept.

In order to promote cloud transparency, the research community concentrated on the definition of assurance methodologies, of which security certification schemes stand out. In this work, we suggested an incremental test-based security certification approach for the cloud that is flexible enough to respond to low-cost cloud events, ongoing system improvements, and changes in certification methodology. When pertinent modifications are noticed, our method modifies existing certificates by reusing their evidence, and it reduces the number of re-certification procedures that must be carried out on certified systems.

REFERENCES

[1] Shireen Nisha, Mohammed Farik “RSA Public key Cryptography Algorithm”, International Journal of Scientific and Technolgy Research, Volume-6, Issue 7, pp 187-189, July 2017

[2] M.Preetha, M. Nithya “A study and performance analysis of RSA algorithm”, International Journal of Computer Science and Mobile Computing (IJCSMC), Volume-2, Issue 6, pp 132-133, JUNE 2013

[3] Annapurna Shetty,Sharuya Shetty, Krithika K “Asymmetric Cryptography-RSA and Elgamal Algorithm”- October 2014

[4] Rishav Chatterje,Sharmishta Roy “Cryptography in Cloud Computing-A basic approach to ensure security in cloud”, INTERNATIONAL JOURNAL OF ENGINERRING SCIENCE AND COMPUTING (IJESC), Volume 7,Issue 5, pp 11818-11819,May 2017

[5] Ahmed Albugim, Madini Alassfi, Robert Walters,Gary Wills “Data security in Cloud Computing”, Fifth

International Conference on Future Generation Communication Technologies(FGCT 2016), pp 55-57,October 2016

[6] Santosh Kumar Singh, Dr. P.K Manjhi, Dr. R.K Tiwari "Data Security using RSA Algorithm in Cloud Computing", International Journal of Advanced Research in Computer and Communication Enginerring (IJARCCE),Volume 5,Issue 8,pp 12-13, August 2016

[7] Annapornna Shetty, Shravya Shetty K, Krithika K "Review on Asymmetric Cryptography-RSA and Elgmal Algorithm", International Research of Innovative Research in Computer and Communication Enginerring, Vol-2, Issue 5, pp 99-101, October 2014.

[8] Ravindra Changala, "Data Mining Techniques for Cloud Technology" in International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE),Volume 4, Issue 8, Pages 2319-5940, ISSN: 2278-1021, August 2015.

[9] S. Pearson, "Toward accountability in the cloud," IEEE Internet Computing, vol. 15, no. 4, pp. 64–69, 2011.

[10] A. Sunyaev and S. Schneider, "Cloud services certification,"Communications of the ACM, vol. 56, no. 2, pp. 33–36,February 2013.

[11] M. Anisetti, C. Ardagna, and E. Damiani, "A certification based trust model for autonomic cloud computing systems," in Proc. of IEEE CAC 2014, London, UK, September 2014.

[12] G. Spanoudakis, E. Damiani, and A. Mana, "Certifying services n cloud: The case for a hybrid, incremental and multilayer approach," in Proc. of HASE 2012, Omaha, NE, USA, October 2012.

[13] CSA Security, Trust & Assurance Registry (STAR), Cloud Security Alliance (CSA), https://cloudsecurityalliance.org/star/.

[14] R. Harjani, M. Arjona, A. Mu˜noz, and A. Ma˜na, "Towards an engineering process for certified multilayer cloud services," in Proc. of LAW 2014, New Orleans, LA, USA, December 2013.

[15] C. Criteria, CCRA Supporting Document 2004-02-009 Assurance Continuity, February 2004,

http://www.commoncriteriaportal.org/files/supplements/2004-02-009.pdf.

[16] M. Anisetti, C. Ardagna, and E. Damiani, "A low-cost security certification scheme for evolving services," in Proc. Of IEEE ICWS 2012, Honolulu, HI, USA, June 2012.