From Security to Assurance in the Cloud: A Survey
从安全到云中的保证：一个调查

第一节

Cloud tenants can use cloud resources at lower prices, and higher performance and flexibility, than traditional on-premises resources, without having to care about infrastructure management.Even though cloud computing provides all these benefits, a number of potential users are still reluctant to adopt it. 与传统的本地资源相比，云租户可以以更低的价格、更高的性能和灵活性使用云资源，而不必关心基础设施管理。 尽管云计算提供了所有这些好处，但许多潜在用户仍然不愿意采用它

论文背景

Lack of security is one of the main reasons discouraging customers and business owners from adopting cloud solutions.缺乏安全性是阻碍客户和企业主采用云解决方案的主要原因之一。

待解决的问题

第二节

We describe our cloud security taxonomy that consists of three main categories and is based on the when, where, what, and how approach. 作者描述了我们的云安全分类法，该分类法由三个主要类别组成，并基于时间、地点、内容和方式方法。

When focuses on the timeframe in which a given solution has been proposed.什么时候侧重于提出特定解决方案的时间框架。

Where relates to the attack surface that is the target of a given security and assurance solution?攻击面与特定安全和保障解决方案的目标有什么关系?

What refers to the property a given security and assurance solution considers.什么指的是一个给定的安全和保证解决方案所考虑的属性。

How considers the way in which a given solution increases security and assurance of the cloud, or in other words by which mechanisms a given security property is supported.如何考虑给定的解决方案如何增加云的安全和保障？哪些方面可以提高云的安全性和保障性，或者换句话说，通过哪些机制可以支持给定的安全属性 支持。

—When: May 2014.
—Where: tenant-on-tenant attack surface.
—What: integrity.
—How: the specific cryptosystem used to strengthen integrity of the data storage.
-时间。2014年5月。
-地点：租户对租户的攻击面。
-什么：完整性。
-如何：用于加强数据存储完整性的特定密码系统。

第三节

Section 3 presents cloud-specific vulnerabilities, threats, and attacks.作者介绍了特定于云的漏洞、威胁和攻击

First, they claim that attacks targeting the interactions between users and services are similar to the ones known for traditional distributed communications (e.g., Denial of Service – DoS, SQL injection, Cross Site Scripting – XSS). However, attacks proper of a cloud environment also involve interfaces managed by the cloud provider. Then, they identify six attack surfaces that are used, possibly in a combination, to perform an attack. Finally, they describe some successful attacks on sample cloud environments.首先，他们声称针对用户和服务之间交互的攻击与传统分布式通信（例如拒绝服务——DoS、SQL注入、跨站点脚本——XSS）中的攻击类似。然而，云环境本身的攻击也涉及由云提供商管理的接口。然后，他们确定了六个攻击面，可能组合使用以执行攻击。最后，他们描述了一些针对示例云环境的成功攻击。

第四节

Provides an overview of existing security solutions. 作者概述了现有的安全解决方案

We have classified cloud security approaches according to the taxonomy of security techniques discussed in Section 2: encryption, signature, access control, IDS/IPS, authentication, trusted computing.作者根据第2节中讨论的安全技术分类法对云安全方法进行了分类：加密、签名、访问控制、IDS/IPS、身份验证、可信计算。

第五节

Discusses assurance techniques for cloud security verification, testing, monitoring, and certification.作者讨论了用于云安全验证、测试、监控和认证的保证技术。

In this section, we survey approaches to the verification and validation of cloud infrastructures. These categories of solutions focus on increasing trust in the cloud infrastructure, can target all levels of the cloud stack, and aim to empower cloud users.在本节中，作者将调查云基础设施的验证和验证方法。这些解决方案类别侧重于增加对云基础设施的信任，可以针对云堆栈的所有级别，并旨在增强云用户的能力。

第六节

Presents a summary of the survey results on the basis of the proposed methodology, highlights our recommendations for next-generation security and assurance solutions, and draws our conclusions.作者根据提议的方法对调查结果进行总结，重点介绍我们对下一代安全和保障解决方案的建议，并得出我们的结论。

结论

If we consider security techniques, 34.8% target confidentiality property (highest), while only 8% target availability property (lowest). The remaining techniques almost equally target integrity, authenticity, and privacy properties (between 17.9% and 21%). Ifwe consider assurance techniques, their distribution is more homogeneous among classes of properties, probably because they have been applied to cloud environments only recently: 29.8% for integrity (highest) and 15.8% for privacy (lowest).如果我们考虑安全技术，34.8% 的目标是机密性（最高），而只有 8% 的目标是可用性（最低）。其余技术几乎同样针对完整性、真实性和隐私属性（介于 17.9% 和 21% 之间）。如果我们考虑保证技术，它们在属性类别中的分布更加均匀，可能是因为它们最近才应用于云环境：完整性为 29.8%（最高），隐私为 15.8%（最低）。

建议

Widespread adoption of cloud computing requires security and assurance solutions increasing the trust of cloud users in the cloud itself and in cloud providers.云计算的广泛采用需要安全和保证解决方案，以增加云用户对云本身和云提供商的信任。

we claim that introspection, which is the capability of a cloud provider of examining and observing its internal processes, is not the only concept that matters when considering cloud security. In fact, the concept of out-rospection, that is, empowering customers and service providers with the ability to examine and observe cloud's internal processes impacting on (the security of) their activities/applications/data, is also of paramount importance.我们声称内省是云提供商检查和观察其内部流程的能力，并不是考虑云安全时唯一重要的概念。事实上，外省的概念，即赋予客户和服务提供商检查和观察影响其活动/应用程序/数据（安全性）的云内部流程的能力，也至关重要。

We claim that an increased cloud transparency can help the security management problem, supporting both introspection and outrospection.我们声称，增加云的透明度可以帮助安全管理问题，支持内省和外省。

Cloud back-end data represent a hidden treasure over which one can build new services, and improve cloud functionality, security, and assurance.云后端数据代表了一个隐藏的宝藏，人们可以通过它构建新的服务，并改进云功能、安全性和保证。