Security in the Skies

Cloud computing security concerns, threats, and controls

Mano Paul, CSSLP, CISSP, AMBCI, MCAD, MCSD, Network+, ECSA

Introduction

The Internet, often represented as a cloud in architectural diagrams, has changed the way of life for both the individual and businesses. This whitepaper highlights the security concerns that are evident in cloud computing, with particular focus on information assurance, and provides strategies to adopt when evaluating cloud service providers and when designing, developing, and deploying applications that will operate in the cloud. It also gives guidance on what some of the next steps need to be for secure cloud computing.

What is Cloud Computing?

Cloud computing is one of the most highly discussed topics within the typical organization, according to the 2011 (ISC)² Global Information Security Workforce Study (GISWS) conducted by Frost and Sullivan. But what is cloud computing? Is it a silver lining in computing, or is it a harbinger of an impending perfect storm? Because the cloud computing paradigm is still evolving, a common definition remains a work-in-progress. The most widely accepted current definition for cloud computing is what the National Institute of Standards and Technology (NIST) developed:

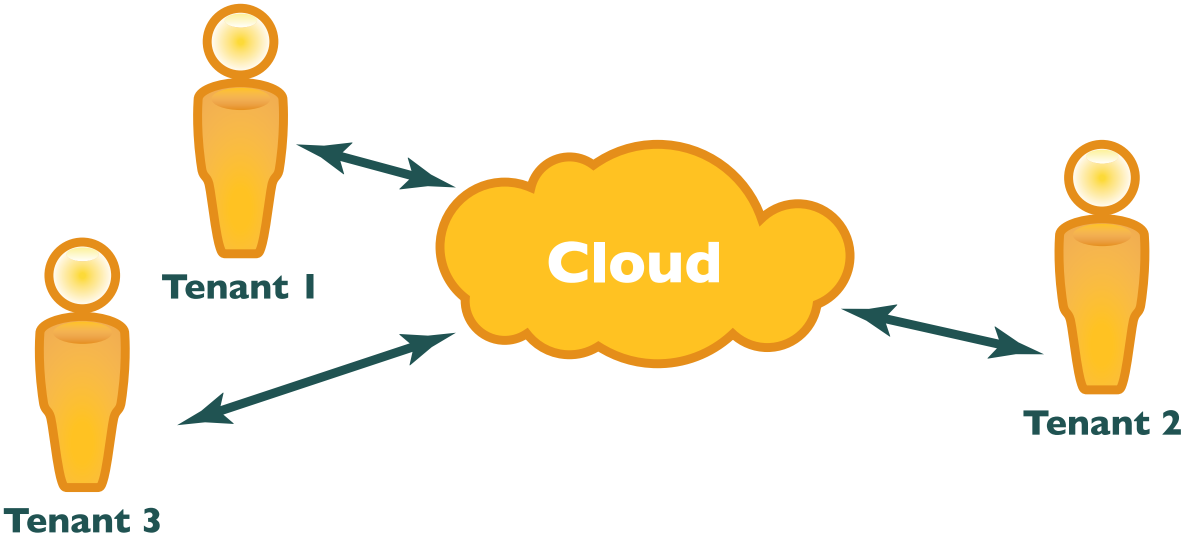
Cloud Computing – A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Architecture and Service Models

> *"The three primary service models in cloud computing are IaaS, PaaS and SaaS"*

The cloud computing architecture is primarily a multi-tenant, service based architecture. It has a distinct consumer front-end and the provider cloud back-end which provides services to the multiple consumers (also referred to as clients of tenants), as shown in Figure 1. The front-end is often just browser based.

Figure 1. Multi-Tenant Cloud Computing Architecture



There are three primary service models that are prevalent in cloud computing. These include Software as a Service (SaaS) in which software applications are provided by the cloud, Platform as a Service (PaaS) in which the cloud provides hardware resources such as virtual machines which can be loaded with user operating systems and software, and Infrastructure as a Service (IaaS) in which infrastructural components are provided by the cloud.

Types of Clouds

The main types of clouds are one or more of the following: public, private, community, or hybrid. In a public cloud, the provider sells their cloud services to multiple clients or tenants that are unrelated. The client is completely at the mercy of the provider to secure its data, applications, and systems, and has little or no control over assurance activities. A private cloud, on the other hand, is a dedicated cloud where the provider supplies cloud services on behalf of the client. In most cases, the client organization is also the provider of the cloud services. In a private cloud, the client has maximum control of assurance activities. A community cloud is more or less an in-between model. It leverages the benefits and risks of both the public and the private cloud. Like the public cloud, there is multi-tenancy, but, unlike a typical public cloud, the tenants are related entities. The clients have common needs, in other words, and the assurance activities are built on client requirements. Finally, there is the hybrid cloud. A hybrid cloud combines two or more deployment models. The assurance mechanisms and controls can be more granular. For example, sensitive and proprietary information can be hosted in the private cloud while projects that relate to the client's industry can be hosted and serviced by a community cloud.

Why Cloud Computing?

Before the adoption of cloud computing, organizations bought and "owned" their physical servers and information technology (IT) infrastructure and systems. Now, with cloud computing, organizations can "rent" infrastructure, platform, and application (as services), and pay for only what they need and use. This rent-as-you-need (on demand, *ad hoc*, or elastic) characteristic of cloud computing makes it very similar to the utility services in the energy sector. It also makes cloud computing very attractive to organizations from a cost perspective. Instead of having to allocate the budget for capital expenditure (CapEx), the financial resources can be more granularly managed and provisioned toward operating expenditure (OpEx). In addition to cost savings, cloud computing also brings with it interoperability between heterogeneous systems and applications as business functionality is abstracted and exposed using application programming interfaces (APIs), allowing clouds to work together. Cloud computing also provides portability as workload can be distributed, device independence as users see the applications and not the computer devices, fluidity and economies of scale as computing resources can be dynamically provisioned, metered usage, ubiquitous computing, and version integrity.

Inevitability of the Cloud

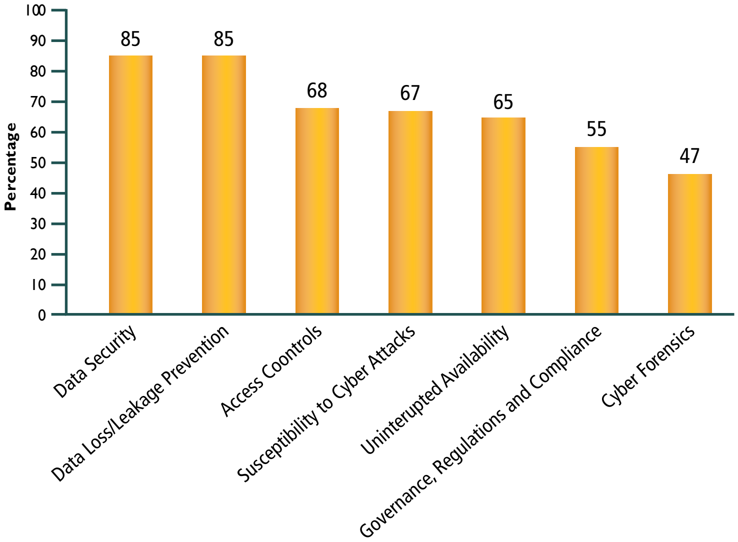
While many organizations are still contemplating the adoption of the cloud for their computing needs, many have already done so. The (ISC)² GISWS reports that more than 50 percent of information security professionals surveyed reported having private clouds in place, and more than 40 percent of respondents reported using SaaS. The question is not if but *when* your organization starts using cloud computing for its needs. This is because cloud computing brings with it many of the above-mentioned benefits. But cloud computing also brings with it associated risks. Just as the Chinese word for "opportunity" can also be used as the word for "crisis", cloud computing which is regarded as an enabler for creating powerful, scalable, and on-demand computing organization, can also be seen as a source of crisis when it comes to the assurance (security) guarantees for its tenants. One thing is for certain and that is that the computing in the cloud is inevitable. The question that remains to be answered is "Will your organization be positioned to securely do business in the cloud?"

"Cloud computing: Opportunity or Crisis?"

Security Concerns in Cloud Computing

While cloud computing has the potential to make IT operations leaner and less expensive, many of the respondents of the 8th annual Global Information Security survey that was published in the CIO magazine have qualms about security, and more than 60 percent of the respondents admitted to having little to no confidence in the ability to secure assets that are placed in the cloud. The findings of the (ISC)² GISWS highlight seven security concerns as shown in Figure 2.

Figure 2. Security Concerns in Cloud Computing



These range from data disclosure protection, ranking as the number one concern, to the inability to support forensic investigations. In this section, we will cover the security concerns with cloud computing and the necessary protection mechanisms that must exist. Uncle Ben's advice to Peter Parker from Spiderman – "With more power comes more responsibility" – is apt advice in today's cloud computing "Webified" world.

Data Security

The primary security concern in cloud computing is data disclosure to unauthorized systems or personnel. When an organization's data is placed in what seems to be a nebulous cloud, the data owner (tenant) is in the inside of the organization while the data custodian (provider) is on the outside, making it a challenge to control data access. It is therefore crucial to ask the following questions to the provider: "Who will have access to your organizational data?", and, "How will access be restricted to only authorized personnel or systems?" It is also crucially important to validate the claims made by the provider.

The format in which data is stored is very important as well. Sensitive and privacy data must not be stored in clear text format. The data needs to be protected using cryptographic protection mechanisms such as encryption (if original value needs to be resynthesized) or hashing (if original value need not be resynthesized). When data is stored in cipher text format, additional storage requirements need to be estimated and planned. The key used for encryption/decryption needs to be protected as well. And to harness the scalability power of the cloud, the applications that operate in the cloud need to be cryptographically agile. In other words, applications need to be designed in such a manner that the swapping out of keys and the replacement of weaker algorithms are significantly easy to do. Keys must not be hardcoded within the API itself, but instead supplied from a source that is configurable and secure.

In order to facilitate easy migration in the cloud, data storage considerations must also factor in the metadata of the network segment and the application. The network segment must have perimeter devices controlling the information, such as the firewall (virtual), switch, router and load-balancer metadata. The metadata for each application within that network segment needs to be recorded as well. This metadata hierarchy must be maintained and reviewed periodically for contextual accuracy because applications can be moved in and out of the cloud within a network segment.

Data Loss or Leakage Prevention

When infrastructure and systems are provisioned dynamically, it is likely that the data that resides on that shared pool of resources can be leaked to entities that have access to those same infrastructural components. One element of confidentiality assurance is the ability to dispose data securely. In clouds that house storage media not controlled by the tenant, verification of data disposal mechanisms so that there is no remanence is crucial. Since magnetic flux degaussing and physical destruction (shredding) of data at "rest" are not viable options in the model of cloud computing, as the storage media will need to be provisioned again, one must resort to the weakest form of data disposal, which is overwriting (or formatting). Overwriting, though providing the least amount of assurance, is a practical solution in the cloud.

Access Controls

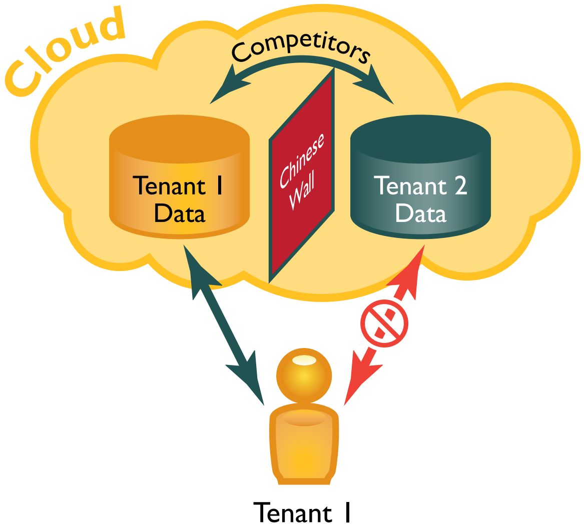
Next only to confidentiality assurance, access control is the most important security concern in the model of cloud computing. This is particularly true when applications and data are hosted in a public cloud. When multiple tenants are supported by a cloud, then the scope of any breach is not contained to a single tenant.

> *"Connected applications in the cloud may allow for unintended connections and unauthorized access"*

The breach of an application in a shared hosted cloud could result in the breach of other applications that use the same pool of resources in that cloud. Connected applications in the cloud may allow for unintended connections and unauthorized access.

When data and systems are hosted in shared hosting environments, access control to data, data privacy and data separation become crucial. The provider should be required to show evidence of the implementation of Brewer & Nash's non-conflict-of-interest Chinese wall model, which prescribes that data from one tenant should be off limits to individuals who could be considered competitors of the tenant, as shown in Figure 3. Appropriate access control lists (ACLs) should be in place to restrict the access to information in such situations. Systems need to be hardened so that they are not susceptible to exploits. Single Sign On (SSO) solutions in the cloud can be a weak link if the system is not designed with security in mind.

Figure 3. Chinese Wall Security Model in the Cloud



Susceptibility to Cyber Attacks

The cyber threats that are observed in the model of cloud computing are not that different from the traditional mode of computing. Both from a programming as well as from a hosting perspective, focus on security is required. The Cloud Security Alliance's publication entitled "Top Threats to Cloud Computing" mentions seven top threats. These include the abuse and nefarious use of computing resources using cracking techniques and malware, insecure application programming interfaces, malicious insiders, shared technology vulnerabilities such as virtualization exploits of the hypervisor and cloud bursting which is characterized by the inability of the cloud to handle spiked demands, data loss/leakage, hijacking of accounts, services and traffic, and an unknown risk profile of the provider due to the general lack of transparency into the provider's inner workings, processes, and procedures.

Because the cloud allows for anonymity, threat agents including malicious insiders are more prone to conduct their nefarious activities with relative impunity. The detection of unauthorized changes in infrastructures, platforms, and software which are not owned and controlled by the data owner is a major challenge. The cloud computing model can also prove to be very lucrative to attackers who aim at conducting man-in-the-middle (MITM) attacks. When software is developed as a service, the software itself is often engineered by abstracting and encapsulating business functionality into contract based services that are exposed using discoverable and invocable application programming interfaces (APIs). Such exposure can lead to scanning and enumeration attacks where an attacker can invoke APIs that are restricted.

Stronger passwords that are not easily guessable or prone to dictionary brute force attacks must be enforced using an implementable identification and authentication policy. User and session tokens that are used for impersonation and delegation need to be protected when they are transmitted by using secure transport (SSL/TLS) and network (IPSec) layer protection mechanisms to assure confidentiality of data in motion and mitigate hijacking and MITM attacks.

It is essential to understand the dependency chain of the APIs so that insecure APIs that allow for clear text authentication, inflexible access control, and limited monitoring and auditing are not used. Another aspect to consider is that proprietary custom APIs can promote vendor lock-in and dependency, and so a return on investment (ROI) when choosing to use providers with proprietary APIs must be done before a selection is made. Identity management with auditing to assure non-repudiation can reduce malicious insider threats. Defense-in-depth strategies and implementations that include sandboxing and hardening are necessary to mitigate the vulnerabilities of shared technology. Data classification, labeling, and data loss prevention (DLP) technologies can be useful in addressing data loss/leakage. But data disposal strategies must be implemented to adequately provide data loss/leakage protection. The provider's internal processes and procedures must be like a glass house to the tenant.

> *"The provider's internal processes and procedures must be like a glass house to the tenant."*

Uninterrupted Availability

Cloud computing has an impact on the availability tenet of security. There are two main schools of thought when it comes to the availability of resources in the cloud computing model. On one hand, one may argue that because the processing load is distributed in the cloud, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks cannot cause significant damage in the cloud. On the other hand, the consumer of the provider's services will still be liable to bear the cost in this pay-per-use model of computing. This cost may quite easily be greater than the cost of downtime caused by the DoS or DDoS attacks. Additionally, the centralization of cloud services can reduce the attack surface but this could also create a single point of failure and so layered defense strategies are essential.

According to the NIST definition of cloud computing, one of its important characteristics is that it is a measured service. Before entering into a relationship with a cloud service provider, get a clear understanding of the service level agreements (SLAs). It is very important that these SLAs take into account the security requirements before any acquisition decision is made. It is also very important that capacity estimation for growing data needs, and redundancy with backup requirements, are carefully planned and architected. The redundancy on-premise and minimum uptime must be specified explicitly in the service level agreement (SLA).

> *"The redundancy on-premise and minimum uptime must be specified explicitly in the service level agreement (SLA). "*

Governance, Regulations and Compliance (GRC) in the Cloud

Two of the biggest concerns that the adopters of cloud computing have is their uncertainty in enforcing security policies at the provider site, and their inability to support compliance audits in the cloud. Though the assurance responsibilities are spread between the cloud service provider and the consumer (tenant), since adequate governance frameworks and regulations are still lacking, the onus is on the side of the consumer to not only verify the existence of adequate protection mechanisms, but in some cases to be responsible for the protection mechanism themselves. For example, Amazon essentially requires that the user or enterprise consumer handle all data encryption and key management, while Amazon provides services for data recovery and auditing. At no time should governance, risk, and compliance activities be outsourced. The Cloud Security Alliance is a commendable undertaking that aims to establish and promote best practices in the cloud.

> *"Not only must due diligence be in place when operating in the cloud, but due care must be demonstrable."*

Not only must due diligence be in place when operating in the cloud, but due care must be demonstrable. The responsibility is also on the cloud service provider to assure the consumer of their security control measures, while at the same time balancing it with security transparency, alleviating the security and privacy concerns of consumers when operating in the cloud. Insight into the inner workings and risk profile of the cloud providers' processes and applications is necessary for assuring the needed IT governance and demonstrating due diligence. At no time should the cloud solution be a black box but instead it must be a glass house for the consumer to be able to conduct review periodically. Compliance management includes validation of the cloud providers' assurance claims. While contracts may be indicative of due diligence, they do not necessarily demonstrate due care. Validation and verification activities that assure that the cloud provider is following claimed security practices and risk management strategies, properly tacks due care on to due diligence.

> *"At no time should the cloud solution be a black box."*

Cyber Forensics in the Cloud

The elasticity of the cloud, where users pay only for what they need on demand, provides challenges to a cyber forensics investigator, since resources such as disk space and memory that are allocated to one's organization today may be gone or overwritten by tomorrow, or, even worse, allocated to someone else (including potentially your competitor). Additionally, the lack of understanding of the underlying infrastructure in the IaaS model makes it difficult, upon a breach, for an investigator to gather evidence. With blurred ownership boundaries, the collection of physical evidence using static and live forensic tools from virtual environments is a challenge.

Cyber forensics must take into account the controls, such as firewalls, event and content logs, and IDSes, on both the tenant's side as well as the provider's side. Visualization of physical and logical data locations becomes a necessity in cloud cyber forensics.

Personnel Security Issues

When it comes to cloud computing, as with any other technological trend or model, the success hinges on the people. Administrative controls such as background screening and checks are a must-have since cloud vendors often use third parties to host infrastructure, platforms, and applications. These third-party hosts can potentially hire people without appropriately screening their backgrounds. Since it is unlikely that you will conduct background checks yourself on third-party personnel, you must request evidence of assurance that the cloud provider meets stringent criteria and in-depth auditing standards, such as the SAS70.

> *"Education and training are crucial for the success of any cloud computing security strategy."*

Education and training are crucial for the success of any cloud computing security strategy. According to the (ISC)^{2} GISWS, cloud computing illustrates a serious gap between technology implementation and the skills necessary to provide security. More than 70 percent of the professionals who participated in the study reported the need for new skills, not just incremental advances, to properly secure cloud-based technologies. The findings from this study also indicate that the skills professionals report as necessary for cloud computing are different from traditional security skills, and a detailed understanding of cloud computing and associated technologies was desired, followed by a demand for specialized skills in contract negotiation.

Where to From Here?

The next steps to ensure that cloud computing is secure in the future is to standardize the cloud. Until standards mature, the Standards Acceleration Jumpstarting Adoption of Cloud Computing (SAJACC) process developed by NIST can help with testing cloud system requirements. Some of the emerging cloud standards include the Open Cloud Manifesto, Open Virtualization Format, Open Cloud Computing Interface, and the Trusted Cloud. The Open Cloud Manifesto is a set of principles that aims at making the cloud interoperable. It is supported by 300-plus vendors who provide a high degree of transparency into their operations. The Open Virtualization Format specification that is proposed by the Distributed Management Task Force aims at making virtualization simpler by having vendors agree to virtual machines' metadata formats. The Open Cloud Computing Interface that is proposed by the Open Grid Forum aims at creating a standardized application programming interface for cloud infrastructure systems. The Trusted Cloud is a set of security standards for cloud computing from the Cloud Security Alliance.

The Cloud Security Alliance takes a holistic approach to cloud security. It has revised the Cloud Controls Matrix (CCM) which provides fundamental security principles to guide cloud vendors. The CCM can be used by clients to assess the overall security risk of the cloud service provider. It is comprehensive and takes a risk-based approach to address threats and vulnerabilities in the cloud, taking into account the business requirements for information security as well. The CCM aims at providing a common criteria and framework for assessing cloud service providers.

On a final note, it is important to recognize that partnership between the government and the private sector is necessary to tackle the security concerns in the cloud.

Table 1. Cloud Computing Security Concerns, Threats and Controls

Security in Cloud Computing		
Concern	**Threat**	**Control**
Data Security	Disclosure to unauthorized systems or personnel	Cryptographic protection such as encryption or hashing of sensitive / privacy data Cryptographically agile applications
Data Loss/Leakage Prevention	Data loss/leakage and data remanence	Secure data disposal Overwriting (formatting) of storage media. Data classification and labeling Data Loss/Leakage Prevention (DLP) technologies
Access Controls	Unauthorized access	Access Control Lists (ACLs) Chinese Wall Hardening
Abuse and Nefarious Use of Computing Resources	Cracking Malware	Stronger authentication mechanisms Secure transmissions (tunneling) Hardened infrastructure, platforms and applications
Insecure and Proprietary APIs	Clear text authentication Inflexible access control Limited monitoring and auditing Vendor lock-in	Understand the dependency chain of APIs Deprecate insecure APIs Perform ROI exercise for proprietary APIs
Shared Technology Vulnerabilities	Hypervisor exploits Cloud bursting	Sandboxing and Hardening Resource planning and provisioning Defense-in-depth
Hijacking of Accounts, Services and Traffic	Disclosure to unauthorized systems or personnel	Session management Secure transmissions (tunneling)
Provider's Risk Profile Unknown	Provider's inner workings Processes and procedures are a black box	Periodically assess provider's risk profile Verify and validate provider's assurance controls claims
Uninterrupted Availability	Denial of Service (DoS) Distributed Denial of Service (DDoS) Uptime uncertainty	Capacity planning Redundancy and Backup Performance and Uptime requirements in Service Level Agreements (SLA)
Governance, Regulations and Compliance	Uncertainty in enforcing security policies at provider's site Inability to support compliance audits	Establish contracts that are enforceable Periodically assess provider's risk profile Verify and validate provider's assurance controls claim
Cyber Forensics	Collection of evidence in a dynamically provisioned environment is a challenge Lack of understanding of provider's infrastructure to collect evidence successfully	Visualization of physical and logical data locations Cryptographically agile applications
Personnel Security	Malicious Insider Insider attacks	Identity management with auditing to assure non-repudiation Background screening checks Awareness, Training and Education

Conclusion

Cloud computing is one of the most discussed topics in the computing industry today. This multi-tenant service-based architecture provides the infrastructure, platform, and/or software as a measured service to multiple consumers (tenants) on demand. Consumers of these services rent services as they need and pay for only what they use, making cloud computing very attractive to organizations from a cost perspective. The cloud also promotes interoperability and portability. The different types of clouds that are most prevalent include public, private, community, and/or hybrid clouds.

While the model of cloud computing brings with it several advantages, it also brings certain risks. Security concerns in cloud computing range from data security and data loss/leakage prevention to cyber forensics challenges in the cloud. The predominant security concerns and controls to design and implement in cloud computing are presented in Table 1. More work to ensure that the cloud computing model is secure is necessary. The government and the private sector must work hand in hand to address the security concerns of this influential trend. Leaving these concerns unaddressed will convert this opportunity for leaner and efficient computing into a crisis. With more power comes more responsibility, and in order to ensure a secure future, we must holistically address the cloud computing security issues today, for it is very likely that cloud computing will be the way that IT computing happens, at least in the near future.

> *"The cloud has moved in and it is here to stay. Will your organization be ready for a rainy day?"*

About (ISC)²®

(ISC)² is the largest not-for-profit membership body of certified information security professionals worldwide, with over 70,000 members in more than 135 countries. Globally recognized as the Gold Standard, (ISC)² issues the Certified Information Systems Security Professional (CISSP®) and related concentrations, as well as the Certified Secure Software Lifecycle Professional (CSSLP®), Certified Authorization Professional (CAP®), and Systems Security Certified Practitioner (SSCP®) credentials to qualifying candidates. (ISC)²'s certifications are among the first information technology credentials to meet the stringent requirements of ANSI/ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel. (ISC)² also offers education programs and services based on its CBK®, a compendium of information security topics. More information is available at **www.isc2.org.**

About the Author

Mano Paul, CSSLP, CISSP, AMBCI, MCAD, MCSD, Network+, ECSA is CEO and President of Express Certifications and SecuRisk Solutions, companies specializing in professional training, certification, security products and security consulting. His security experience includes designing and developing software security programs from Compliance-to-Coding, application security risk management, security strategy and management, and conducting security awareness sessions, training, and other educational activities. He is currently authoring the Official (ISC)² Guide to the CSSLP, is a contributing author for the Information Security Management Handbook, writes periodically for Certification, Software Development and Security magazines and has contributed to several security topics for the Microsoft Solutions Developer Network. He has been featured in various domestic and international security conferences and is an invited speaker and panelist in the CSI (Computer Security Institute), Catalyst (Burton Group), TRISC (Texas Regional Infrastructure Security Conference), SC World Congress, and the OWASP (Open Web Application Security Project) application security conferences. He can be reached at **mano.paul@expresscertifications.com** or **mano.paul@securisksolutions.com.**

References

Definition of Cloud Computing by the National Institute of Standards and Technology (NIST).

2011 (ISC)² Global Information Security Workforce Study

8th Annual Global Information Security Survey, CIO

Clash of the Clouds, Kim S. Nash. CIO Magazine. May 2010

CSO Magazine, November 2010. Security Questions for Big Clouds – Gregory Machler

Clearer Definition, New Metrics for Cloud Security. CSO, Jan 2010. Ariel Silverstone

Cloud Assurance Still Missing. Allan Carey

Cloud Computing for the Federal Community. Hannah Wald. Information Assurance Technology Analysis Center (IATAC) Newsletter. Volume 13 Number 2. Spring 2010.

Establishing Trust in Cloud Computing. Dr. Bret Michael and Dr. George Dinolt. Information Assurance Technology Analysis Center (IATAC) Newsletter. Volume 13 Number 2. Spring 2010.

Turbulence in the Clouds. Peter Fretty. Infosecurity Professional. Issue Number 12. Pp 8-11.

Cyber Forensics in the Cloud. Scott Zimmerman and Dominick Glavach. Information Assurance Technology Analysis Center (IATAC) Newsletter. Volume 14 Number 1. Winter 2011.

Top Threats to Cloud Computing, Version 1.0. Cloud Security Alliance.

(ISC)^2®