EVS: A Cloud Services Information Security and Privacy Eligibility and Verification System

Fahad F. Alruwaili and T. Aaron Gulliver

Department of Electrical and Computer Engineering
University of Victoria,
P.O. Box 1700 STN CSC
Victoria, BC V8W 2Y2 Canada
{fruwaili,agullive}@uvic.ca

Abstract—In recent years, cloud computing services have evolved as a new paradigm for delivering computing resources that are dynamic and customizable, and provide high performance. Many organizations are migrating their information technology (IT) systems to the cloud due to the technological and economic opportunities it provides. However, security and compliance concerns exist that can undermine confidence and trust in cloud service providers. To address these concerns, an eligibility and verification system (EVS) is proposed to improve confidence and trust in cloud service providers, and the cloud community as a whole. The EVS architecture is designed to verify the existence of information security, privacy, and compliance (ISPC) controls in cloud services. This is achieved via several measures, i.e. real-time monitoring, physical verification, and an in-depth five domain ISPC control matrix. This system establishes a foundation for promoting transparent, trusted, and compliant cloud services.

Keywords—Compliance Verification, Cloud Information Security, Eligibility System, Control Matrix, Information Privacy.

I. INTRODUCTION

Cloud computing services are considered to be the next generation technology based on a distributed computing platform that enables on-demand and dynamic provisioning of information technology (IT) resources. These services are offered as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), and leverage virtualization and internet technologies. Cloud IT capabilities are delivered to customers using a pay-as-you-go model, i.e., cloud customers can purchase resources as required, enabling agile adaptation to new IT demands. Cloud resource delivery eliminates the burden of establishing an IT system with the associated infrastructure and personnel [1], [2].

Currently, cloud service providers guarantee the quality of their services according to service level agreements (SLAs). However, these SLAs lack the technical means of enforcing and verifying the information security, privacy, and compliance (ISPC) required by customers and regulatory bodies [1]. The consequences of not beginning compliant with ISPC internal policies and external regulations could be disastrous for both cloud service providers and customers [2]. The effects range from lost reputation, customer trust and confidence, to lawsuits and financial penalties. Thus, organizations wanting to migrate to the cloud have significant responsibilities when selecting a cloud service provider. The responsibilities are even greater for cloud service providers to ensure compliance with customer ISPC requirements.

Having control of cloud services allows providers to abstract the ISPC control management for their customers. Typically, the degree of control that customers have if they rent public cloud services is minimal [3]. Cloud customers can have more control over private cloud services, but there are other aspects to cloud control. For example, the location of cloud data and services can greatly impact data security and legal concerns [4]. In addition, it may be unrealistic to use public cloud services if the data is subject to legal restrictions and ISPC requirements unless cloud providers can furnish compliant and certified services. The many challenges for cloud providers in adapting ISPC requirements to abstract architecture necessitate new security...
models and frameworks. In this paper, a system is presented which can verify and monitor compliance with these requirements.

II. CUSTOMER MOTIVATION AND REQUIREMENTS

Cloud computing has emerged as a cost-effective means of obtaining internet-enabled information technology (IT) services. Despite the benefits of cloud computing services, it is difficult to find the cloud provider best suited to customer requirements [5]. Many organizations have ISPC concerns, and this has created significant research and development in this area [6]. Addressing these concerns requires customer trust and confidence in cloud-enabled services, i.e. software, applications, and infrastructure.

It is often the case that organizations wanting to migrate to the public cloud do not adequately evaluate the information security and data privacy programs of potential cloud providers [7]. In addition, cloud service providers typically only make general terms and practices public, and are reluctant to disclose any details [8]. This has resulted in a significant increase in trusted third party audits [9]. Cloud customers and organizations wanting to adopt cloud services are advised to:

- Select a cloud provider that exercise due diligence in adequately addressing ISPC requirements and concerns. Providers should also follow best cloud information security practices.
- Select a cloud provider that is transparent with regards to ISPC practices, including risk assessment, incident response, and security operations and monitoring.
- Select a cloud service provider that can implement security controls and practices tailored to cloud customers according to their ISPC requirements.

To alleviate customer information security, privacy, and compliance (ISPC) concerns and assist them in selecting the most appropriate cloud service provider, a cloud ISPC eligibility and verification system (EVS) should be employed by a trusted third party to assess cloud providers based on their conformance to the ISPC criteria. Other criteria such as pricing and service features can be incorporated in this system, but the focus here is on ISPC as it is the key to cloud protection. The proposed system combines ISPC policies and controls based on best and widely accepted practices to assess the ISPC services of cloud service providers. Moreover, it allows organizations wanting to migrate their IT systems to the cloud to determine appropriate ISPC services prior to cloud provisioning.

III. RELATED WORK

Despite the increasing acceptance of cloud services, many important security concerns remain unresolved or solved only partially [5]. One of these concerns is the verification and monitoring of ISPC compliance. The only approach related to that proposed in this paper is the automated security compliance tool (ASCT) presented by Zou et al. [10] to verify the compliance of cloud providers. This tool consists of three core components: data collection, verification engine, and user interface. However, it is limited to just access control to cloud services. In addition, no means of providing ISPC compliance are given such as ISPC controls, service linkage for real-time monitoring, historical performance, and compliance records, customer feedback, and compliance services.

Chen et al. [12] proposed an authentication-as-a-service (AaaS) architecture in order to protect sensitive customer information from the cloud provider and other customers. Two-factor authentication is employed based on AaaS generated tokens which provides some degree of trust and anonymity, but this approach is vulnerable to attacks such as distributed denial of service (DDoS). Supriya et al. [13] presented a trust management model to compare cloud service providers in terms of service quality and security. However, this approach is primarily intended to evaluate services and accessibility, and security is not considered in detail. In [13], a compliance solution was provided with location constraints mandated by regulatory authorities. However, only monitoring and tracing of cloud service IP addresses is employed, and these can easily be masked by an attacker, so additional security measures are needed.

IV. ELIGIBILITY VERIFICATION SYSTEM (EVS) OVERVIEW

In this paper, the design science research (DSR) methodology for information systems is employed. This methodology employs a specific set of concepts and principles to develop IT solutions [14], [15]. The main DSR elements are summarized in Table I. It begins with identifying the problem and setting the objectives, which are discussed in Section II. This is followed by designing, developing, and demonstrating the problem, which is presented as the EVS architecture in Section V.

In addition to the DSR methodology, the approach developed in [17] to verify and monitor the selected ISPC controls is employed. This allows potential cloud customers to determine if their acquired services are continuously compliant with the corresponding ISPC controls, which promotes cloud transparency and trust. Further, an ISPC
control matrix is derived from the secure service level agreement (SecSLA) in [18] to assist in control evaluation. The SecSLA specifies the ISPC controls needed to satisfy cloud customer requirements. This is an extension of existing SLA agreements to include ISPC for cloud environments.

<table>
<thead>
<tr>
<th>GUIDELINE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Design</td>
<td>The EVS system is a suitable model for determining provider eligibility and verifying cloud ISPC controls.</td>
</tr>
<tr>
<td>2 Problem Relevance</td>
<td>Despite the benefits of cloud computing services, it is difficult to find the cloud provider best suited to customer requirements [5]. Many organizations have ISPC concerns [6], and cloud service providers typically only make general terms and practices public, and are reluctant to disclose any details [8]. Thus trusted third party trusted audits are required [9]. The objective is to develop a solution which can be adopted by a trusted third party to verify the ISPC controls and cloud provider eligibility.</td>
</tr>
<tr>
<td>3 Design Evaluation</td>
<td>The EVS system is evaluated using an environment which reflects real world situations as a proof of concept.</td>
</tr>
<tr>
<td>4 Contributions to Research</td>
<td>The EVS system provides clear and significant contributions in the area of cloud ISPC.</td>
</tr>
<tr>
<td>5 Research Rigor</td>
<td>The proposed solution relies on rigorous information security methods and models acquired from the results in [17], [18].</td>
</tr>
<tr>
<td>6 Design as a Search Process</td>
<td>The search for an effective cloud eligibility and verification solution requires examining all available approaches to reach a solution.</td>
</tr>
<tr>
<td>7 Research Communication</td>
<td>The insights gained are disseminated to the cloud technology and management communities.</td>
</tr>
</tbody>
</table>

Table 1. Design Science Research (DSR) guidelines.

Incorporating the results in [16], [17] along with the DSR methodology makes EVS an effective tool for cloud customers to obtain information that is verifiable and accountable, and ensures that service providers comply with ISPC requirements. The information provided by the EVS supports the decision making processes for:

- Cloud customers to select the most suitable service provider that is compliant with their ISPC requirements.
- Cloud providers to address missing ISPC components and obtain a competitive advantage in the cloud community.

The EVS allows cloud customers to check the ability of service providers to comply with their ISPC requirements. The EVS user interface (UI) provides ISPC control tables so that potential customers can choose the most suitable controls. The tables are based on detailed ISPC control matrices. The advantages of the proposed approach are:

- Potential customers can verify cloud service provider compliance with ISPC requirements. Informed and trusted decisions can be made based on EVS scores and results.
- Cloud service providers can verify their ISPC eligibility. This encourages cloud providers to become ISPC compliant which may provide a competitive advantage over other providers.

The proposed EVS system encourages cloud service providers to provide trusted and compliant cloud services, and stay current in meeting the requirements of cloud customers. Typically, these requirements fall into one or more of the following areas:

- Information security,
- Data privacy, and
- Compliance with internal policies and external regulatory requirements.

A major reason for adopting the proposed EVS system is to achieve accountable, up to date, verifiable, transparent, and certified results. Thus, the system should be operated, managed, and maintained by a trusted third party. This third party is responsible for the EVS system results, and so is motivated to continuously verify the ISPC controls and closely monitor any changes to them.

V. THE CLOUD SECURITY SYSTEM DEVELOPMENT LIFE CYCLE

In this section, the eligibility and verification system (EVS) architecture is presented. The goal is to provide ISPC compliance verification capabilities as well as real-time monitoring. The EVS architecture is divided into several modules as shown in Figure 1 and described below.
A. Customer-Provider Linkage Service (LS)

The EVS linkage service (LS) is provided to customers and service providers to enable ISPC control verification and real-time updates. It begins when cloud customers select a cloud service provider and relevant services, or a cloud provider links its services to current customers. To establish the LS between a service provider and customer, one party initiates the request and the other validates and accepts the request. The LS function allows each customer to link their cloud services and monitor the associated ISPC compliance. The LS produces detailed information which can be compared with that provided by the eligibility index (EI) report discussed in Section V.C.

To terminate a link, the party that initiated the original LS request (link master) can execute a termination process. In addition, the connected party (request receiver), can revoke/terminate the link based on the EVS LS agreement. Figure 2 shows the LS establishment process. The same process is employed to terminate the link.

Consider an EVS system with C subscribed cloud customers. Once a linkage service is established, the compliance status of an associated ISPC control is can be obtained by customer c from cloud service provider p. The status of an ISPC service can be compliant, non-compliant, or temporarily non-compliant, denoted as 1, 0, or -1, respectively. For customer c, the status of their controls over time can be expressed in a 2D matrix given by:

\[
\begin{bmatrix}
I_{S_{c1}} & \cdots & I_{S_{cT}} \\
\vdots & \ddots & \vdots \\
I_{S_{N_c1}} & \cdots & I_{S_{N_cT}}
\end{bmatrix}
\]

where \(n=1,...,N\) denotes a control, and \(t=1,...,T\) denotes time. If the status of a control is temporarily non-compliant, the time for a cloud provider to become compliant is specified in the agreement between the cloud customer and provider. If the status of a control becomes zero, the customer is
informed that the relevant service is no longer compliant and further action is needed.

The real-time monitoring of ISPC controls and their compliance is governed by the LS update agent. This is typically done via service provider system logs and regular ISPC control assessments. The LS update agent is also responsible for coordinating updates among EVS system modules, i.e. historical records and performance (HRP) database, eligibility checks (ECs), and compliance monitoring (CM), to maintain up-to-date verification and eligibility data.

**Figure 2.** The EVS linkage process.

### B. Compliance Monitoring (CM)

The compliance monitoring (CM) module operates as a dedicated session for each customer to monitor their ISPC requirements. The following are required to begin a session:

- The customer must be subscribed to the EVS system.
- The customer must be linked to at least one cloud service provider.
- The service provider must exist in the EVS system.
- The customer must have selected the ISPC controls for the linked services.

Cloud service providers that subscribe to the EVS system must keep their ISPC logs current to maintain their eligibility status (ES). The CM sets a schedule for cloud providers to update their logs. If an update is not received, the CM sends a message to immediately update the related ISPC records in order to remain compliant. Otherwise, the CM will change the status of the associated services that were previously compliant to temporary non-compliant until an update is received. If no update is received after a specified time period, the status of these services will be changed to non-compliant. The CM will also notify the affected parties, i.e. the linked cloud customers, and inform them once the cloud services return to compliant status.

As cloud customers can have different ISPC requirements, a cloud provider may be fully compliant with one customer but not with another. Therefore, CM consists of multiple monitoring sessions that correspond to the EVS services and linked cloud customers.
Change requests are made to the CM by cloud customers to reflect new or revised ISPC requirements. The CM then notifies the linked cloud service providers of the changes. This should not affect the ES of the cloud providers until they have been approved by the providers and customers, and are in effect. The approval process is conducted by the EVS agent which is responsible for verifying the authenticity and existence of the changes, usually via ongoing ISPC control assessments, remote access, and if necessary site visits.

C. Cloud Service Provider Historical Records and Performance (HRP) Database

The historical records and performance (HRP) database contains information on service provider performance, customer feedback and satisfaction, pricing, third party auditor/assessor evaluations, and monitoring results. EVS customers have access to this database to obtain information on ISPC controls, location and pricing. This allows cloud customers to evaluate their current ISPC activities and refine their decisions to:

- Adopt compliant cloud services.
- Improve the performance and functionality of their ISPC systems.
- Develop new services and products to gain a competitive advantage.

The HRP database is updated based on ISPC changes, periodic monitoring, and ongoing ISPC control assessments. Cloud service provider changes that are not reported and/or reflected in the HRP database can lead to inaccurate conclusions as well as a loss of customer trust and confidence in EVS services. Therefore, this database is designed to ensure it contains accurate and current information. This is achieved by allowing cloud providers to send updates to the HRP at any time. The EVS agent verifies the authenticity and existence of all updates, after which they are added to the database and accessible by the relevant customers.

The ISPC eligibility index (EI) report provides verification of cloud provider conformance with ISPC requirements. The EI is part of the HRP database, but it does not contain detailed information on provider services and their compliance with control requirements (which is the function of the LS). However, it is useful for management who require an overview of the status of potential cloud providers. The EI report also allows customers to easily confirm that their cloud providers are compliant. Cloud service providers are scored on a scale, e.g. 0 to 10, according to their HRP records, where 10 indicates a very compliant and widely accepted service provider, 5 indicates partially compliant, and 0 denotes not compliant with the ISPC control requirements.

D. The ISPC Control Matrix

The ISPC control matrix contains information on the security, privacy, and compliance controls. It maps the ISPC contractual agreement to the set of controls to be applied to the relevant cloud services, i.e. storage, network infrastructure, platform, and applications. For example, a contractual requirement to implement data integrity entails that the intersection between cloud technology, data integrity controls, and cloud storage must be clearly defined. One security control to address this intersection is the implementation of cryptographic mechanisms and intrusion detection and prevention systems. This will protect the integrity of cloud data and alert involved parties of any unauthorized modifications to this data.

Cloud providers and customers use the ISPC control matrix to select the most appropriate ISPC controls. If an ISPC control is new and does not exist in the matrix, the EVS customer can request that a new entry be made. This matrix is based on the previously developed cloud ISPC cubic model [18], [21] that addresses information security and privacy in cloud service level agreements (SLAs). It covers the areas of confidentiality, integrity, availability, and privacy and their application to cloud service models, i.e. IaaS, PaaS, and SaaS. In this paper, this matrix is extended to include compliance so it has five domains to provide comprehensive ISPC coverage. These are confidentiality, integrity, availability, privacy, and compliance. Confidentiality measures are used to prevent unauthorized cloud information access and disclosure. For example, an organization should implement strong authentication methods such as two-factor authentication. User access can also be limited to only the information required to complete a certain task i.e. role based access control. An organization must implement Integrity measures to protect the authenticity of its critical assets from unauthorized modification, e.g. encrypting data. Since cloud resources are prone to attacks such as distributed denial of service (DDoS) that prevent customer access, Availability controls and service level agreements must be in place to address the issues of service interruption and maintenance. Privacy controls should also be identified to protect customer assets, e.g. a policy with a detailed explanation of what is acceptable (and also unacceptable) behavior to ensure security, privacy and compliance. Finally, Compliance controls are those terms and conditions identified in any applicable laws, regulations, contracts, strategies and policies, e.g. ISO27001, PCI DSS, and HIPAA. Customers want to ensure that cloud service providers continuous conform with all compliance requirements.
E. EVS User Interface (UI)

The user interface (UI) provides a simple and practical means for customers to connect to the EVS system. The UI is typically a web portal. It is designed to allow EVS operators to optimize EVS processes and maximize usability. The UI serves both customers and subscribers, i.e., cloud service providers and cloud customers, but other organizations such as auditors and regulatory and legal entities can be given access. The EVS system should have a detailed service agreement with the operating entity i.e., trusted third party. Each subscribed customer should carefully review and accept this service agreement prior to selecting the EVS services. The following are available via the UI:

1. The EVS customer database (CD) allows customers to create a portfolio through a sign-up and validation process. This portfolio consists of the customer details and their preferred ISPC controls. The EVS agent is responsible for verifying portfolios and establishing their authenticity. Subscribed EVS customers receive updates of changes to their preferred ISPC controls.

2. An EVS consultancy service request (CSR) provides either a customer or EVS entity with the information required to review, evaluate, and accept consultancy agreements. These actions constitute a legal commitment, which protects both the EVS entity and customer. For instance, if an EVS entity provides a consultancy recommendation that fails to address the customer ISPC concerns, then it may be liable for any consequences. Conversely, if a cloud customer does not adopt the suggested EVS cloud solutions, the EVS entity will not be liable for any consequences. The CSR consist of:
   a. ISPC control auditing (CA) provided by independent trustees, i.e. accountants, legal entities, and ISPC auditors. An EVS customer is given access to the ISPC report of a cloud service provider only if it has an active relationship with the provider. Otherwise, the cloud service provider can choose not to disclose the audit report to potential customers.
   b. Statistical information (SI) retrieved from the HRP database to provide current and past information on cloud providers such as customer satisfaction, customer feedback, ISPC audit reports, ISPC availability, and ISPC control management.
   c. The eligibility check (EC) which is part of the EVS eligibility service as discussed below. Note that if requested, eligibility information on selected ISPC controls should be analyzed and sent to the customer.
   d. Consultancy reports which are digitally signed and sent to customers.
   e. Mandates for new ISPC controls, in which case additional advisory services can be delivered by the CSR. The CSR can act as a mediator between cloud customers and service providers to deliver the new controls. Once approved and implemented, these controls become new entries in the ISPC control matrix.

The UI should implement information security principles such as least privilege, defense in depth, and fail-safe stance in order to avoid or minimize security issues. The EVS designers should consider these principles early in the UI design and development process. This is critical as failure to adopt appropriate security principles can negatively impact customer confidence and trust [20].

F. EVS Services

The EVS system provides services to customers so they can verify the compliance of cloud service providers according to their ISPC requirements. The system also provides services to providers so they can verify their eligibility to satisfy ISPC requirements. These services are:

1. EVS eligibility service request (ESR)
   a. The cloud service provider selects the desired EVS services

   i. ISPC Eligibility Check (EC)
      1. The provider obtains a detailed description of the ISPC controls.
      2. The EVS agent verifies the existence and status of the ISPC controls.
      3. The EC provides a preliminary eligibility report.
      4. A comprehensive EC report is created, digitally signed and sent to the cloud provider.
      5. The report results are placed in the EVS, i.e. the HRP database, to ensure information is consistent and up-to-date.

   ii. Access to the HRP database
      Subscribed cloud providers have the ability to review their
historical records and performance information. If an error has been made, they can file a request to amend the database.

iii. Access to the EI

Subscribed cloud providers can obtain a summary of the EVS information. This consists of a ranked list of providers in terms of the existence and status of ISPC controls over a specified period of time, e.g. the past two years. The summary is sufficiently comprehensive for providers to make informed decisions on improving cloud services security and privacy compliance.

VI. CONCLUSION

Information security and data privacy violations are serious concerns, and it is important that procedures for avoiding and handling them are developed and adopted [19]. When cloud data falls under regulatory or compliance restrictions, organizations must know if a potential cloud service provider is compliant with their information, security, privacy and compliance (ISPC) requirements prior to cloud deployment and migration. Otherwise, information security, privacy, and regulatory requirements may be violated which can result in a loss of reputation and other serious consequences. Thus, it is expected that organizations will not select a cloud provider without verifying their compliance with the ISPC requirements.

In this paper, a reliable, trusted, and accountable ISPC eligibility and verification system (EVS) was presented. This system is based on a previously developed cloud trusted security model [16] to enable continuous monitoring and auditing by an accredited third party, i.e. 3PCAO or a third party cloud assessment organization. This enables the EVS system to assess the operation of all registered cloud service providers. Eligibility assessment results for cloud providers allow current and potential cloud customers to verify ISPC compliance and other criteria such as ISPC performance, pricing, and customer feedback and satisfaction. This will allow EVS customers, i.e. cloud providers and customers, to make strategic decisions based on current and historical ISPC information.

The EVS system determines ratings and eligibility based on log entries collected securely from the subscribed cloud service providers. EVS agents are used to verify the accuracy of the logs. This is done by remote access of system logs and/or site visits authorized under non-disclosure agreements. The system can be used to verify ISPC controls and compliant cloud services. However, to achieve this goal it must be accepted by the cloud community. The proposed system can also be used by cloud service providers to develop new ISPC initiatives to obtain a competitive advantage over other providers.

REFERENCES


**AUTHOR BIOGRAPHIES**

**Fahad F. Alruwaili** is a member at the Department of Computer Science at the University of Shaqra, Saudi Arabia. He works as an information security and computer networks consultant with over twelve years of practical experience and research development. He earned the BS degree in Computer Engineering from King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2002. In 2008, he received the MS degree in Computer, Information, and Network Security with first class honours from DePaul University, Chicago USA. In 2011, he received the MS degree in Information Systems and Technology from Claremont Graduate University, Los Angeles USA with first class honours. He is currently working towards a PhD degree in Computer Engineering at the University of Victoria, Victoria, BC, Canada. His research interests are in the technical and theoretical aspects of information security and data privacy.

**T. Aaron Gulliver** received the PhD degree in Electrical Engineering from the University of Victoria, Victoria, BC, Canada in 1989. From 1989 to 1991 he was employed as a Defence Scientist at Defence Research Establishment Ottawa, Ottawa, ON, Canada. He has held academic positions at Carleton University, Ottawa, and the University of Canterbury, Christchurch, New Zealand. He joined the University of Victoria in 1999 and is a Professor in the Department of Electrical and Computer Engineering. In 2002, he became a Fellow of the Engineering Institute of Canada, and in 2012 a Fellow of the Canadian Academy of Engineering. His research interests include security, cloud and grid computing, information theory and communication theory, algebraic coding theory, and cryptography.