The Case for Dynamic Security Solutions in Public Cloud Workflow Deployments

John C. Mace, Aad van Moorsel and Paul Watson
The Case for Dynamic Security Solutions in Public Cloud Workflow Deployments

J. C. Mace, A. van Moorsel, P. Watson

Abstract

Many enterprises are currently exploring the potential cost benefits of running applications in public clouds. Enterprises often have global security policies to ensure that its information management conforms to business rules and legal mandates. The location of data storage and application execution therefore becomes a critical issue. The prevalence of Service Oriented Architectures (SOA) means that applications are often composed from a set of services which form a workflow. The concept of running workflow instances on public cloud processing platforms is in its infancy. The scientific community still needs to define the security issues in public cloud workflow deployment and the requirements of possible solutions that will deal with those concerns. This paper aims to address this by exploring the current information security issues of public cloud workflow deployment within an enterprise setting and by identifying core requirements of solutions needed to deal with these challenges. We argue that enterprises would benefit from an automated and dynamic approach when selecting where to execute workflows and store data. This approach would choose what workflows, or subsets of workflows, can be executed in a public cloud environment while ensuring that enterprise security and compliance needs are met.
Abstract

Many enterprises are currently exploring the potential cost benefits of running applications in public clouds. Enterprises often have global security policies to ensure that its information management conforms to business rules and legal mandates. The location of data storage and application execution therefore becomes a critical issue. The prevalence of Service Oriented Architectures (SOA) means that applications are often composed from a set of services which form a workflow. The concept of running workflow instances on public cloud processing platforms is in its infancy. The scientific community still needs to define the security issues in public cloud workflow deployment and the requirements of possible solutions that will deal with those concerns. This paper aims to address this by exploring the current information security issues of public cloud workflow deployment within an enterprise setting and by identifying core requirements of solutions needed to deal with these challenges. We argue that enterprises would benefit from an automated and dynamic approach when selecting where to execute workflows and store data. This approach would choose what workflows, or subsets of workflows, can be executed in a public cloud environment while ensuring that enterprise security and compliance needs are met.

About the authors

John Mace is a Ph.D. student in the Systems research group at Newcastle University where he conducts his doctoral research under the supervision of Prof. Aad van Moorsel in the area of public cloud deployed workflows and their associated information security issues. John completed a BSc (Hons) First Class in Computing Science at Newcastle University in 2010 during which time he received a Scott Logic prize for computer excellence and the School of Computing Science prize for best final year performance. In September 2011, John will commence a 6-12 month internship at HP Research Labs, Bristol, in the Cloud and Security Lab.

Aad van Moorsel is Professor of Computing Science, Director of CS Research at Newcastle University and Director of Centre for Cybercrime and Computer Security. He worked in industry from 1996 until 2003, first as a researcher at Bell Labs/Lucent Technologies in Murray Hill and then as a research manager at Hewlett-Packard Labs in Palo Alto, both in the United States. He joined Newcastle University in 2004 where his research agenda aims at establishing an intelligent enterprise, with a specific focus on trust, privacy and security. The goal is to provide tools to improve IT decision making, if possible based on objective, quantitative methods, eventually fully automated. This involves mathematical modelling, algorithms and service-oriented software implementations.

Paul Watson is Professor of Computer Science, Director of the Informatics Research Institute, and Director of the North East Regional e-Science Centre. He also directs the UKRC Digital Economy Hub on "Inclusion through the Digital Economy". In August 1995 he moved to Newcastle University, where he has been an investigator on research projects worth over 20M. Paul teaches information management on the System Design for Internet Applications Msc and the e-business MSc. In total, Paul has over forty refereed publications, and three patents. Professor Watson is a Chartered Engineer, a Fellow of the British Computer Society, and a member of the UK Computing Research Committee.

Suggested keywords

CLOUD COMPUTING
INFORMATION SECURITY
WORKFLOW
DYNAMIC DECISION MAKING
The Case for Dynamic Security Solutions in Public Cloud Workflow Deployments

John C. Mace, Aad van Moorsel and Paul Watson
School of Computing Science & Centre for Cybercrime and Computer Security (CCCS)
Newcastle University, Newcastle upon Tyne, NE1 7RU, UK
Email: \{j.c.mace, aad.vanmoorsel, paul.watson\}@newcastle.ac.uk

Abstract—Many enterprises are currently exploring the potential cost benefits of running applications in public clouds. Enterprises often have global security policies to ensure that its information management conforms to business rules and legal mandates. The location of data storage and application execution therefore becomes a critical issue. The prevalence of Service Oriented Architectures (SOA) means that applications are often composed from a set of services which form a workflow. The concept of running workflow instances on public cloud processing platforms is in its infancy. The scientific community still needs to define the security issues in public cloud workflow deployment and the requirements of possible solutions that will deal with these challenges. We argue that enterprises would benefit from an automated and dynamic approach when selecting where to execute workflows and store data. This approach would choose what workflows, or subsets of workflows, can be executed in a public cloud environment while ensuring that enterprise security and compliance needs are met.

Keywords—cloud computing; information security; workflow; dynamic decision making.

I. INTRODUCTION

Within an enterprise environment, complex and repetitive processes are often carried out by automated applications. With the prevalence of Service Oriented Architectures (SOA), in-house applications are often composed of a set of re-usable enterprise services which form workflows. Internal storage and processing hardware can often be limited, making workflow execution liable to performance deficits and increased run time. If adequate resources are available they are prone to under-utilisation outside of peak times, and therefore wasted expenditure1.

Amid ever increasing productivity needs, cloud computing provides the ideal environment for executing workflow instances, offering enhanced performance and cost benefits with massively scalable hardware resources, available on demand in a pay-as-you go manner. Despite these benefits, the adoption of public cloud computing is being slowed by its associated security risks and compliance issues [1]. Storing data and running workflows in public clouds often means security management is taken out of the customer’s hands and placed in the control of the cloud provider. This makes it difficult to ensure an enterprise’s information security policies are upheld.

Enterprise workflows may need to handle and process sensitive information, making the security of the processing platforms a necessary concern. Security policies are typically applied to workflows which can make conformance complex, time consuming and error prone, especially for those who are unfamiliar with, or lack concern for, information security issues [6, pp. 76]. But, it is often these same people who choose what to provision on public clouds on a day-to-day basis. This results in potentially insecure workflows and a lack of financial control [1]. An employee under pressure to deliver rapid workflow deployment; and who can provision cloud-based hardware within a matter of minutes, is unlikely to assess the suitability of a cloud’s security controls with the necessary detail, if at all [13]. Although data access control is considered, the controlled deployment of workflow instances to public cloud platforms is not. Controlled cloud resource usage must become a necessary consideration when choosing a cloud deployment strategy, thus placing security controls alongside familiar financial and performance constraints2.

Enacting workflows and storing data in public clouds must be done in a cost effective manner that maintains the information security policy of the data owner. With enterprises still coming to grips with cloud computing, its security and compliance obligations are seen as a ‘grey area’. Furthermore, insufficient runtime auditing techniques of cloud vendor security causes difficulties when ensuring changeable security requirements are met. This lack of transparency coupled with potentially uncontrolled workflows being placed in public clouds means enterprises are often utilising public clouds without an effective data governance strategy3.

The recent paradigm of cloud computing coupled with the new emergence of cloud deployed workflows means the scientific community is yet to define the security issues of deploying workflows in a public cloud setting. Also lacking


is the articulation of solutions, and their requirements, that attend to those issues. This paper aims to address these areas by examining current information security issues of public cloud workflow deployment experienced within an enterprise environment. It goes on to discuss the requirements of possible solutions that would attend to these issues by providing rapid, dynamic and secure workflow deployment. Using these requirements we argue that a dynamic, automated policy-driven approach is needed to monitor and control the current ad-hoc, and often unauthorised, practices of public cloud resource provisioning and workflow deployment. We propose to develop this approach which would dynamically choose what workflows, or subsets of workflows, can be executed in a public cloud environment while ensuring that enterprise security and compliance needs are met. This would bring an enterprise’s public cloud workflow deployments in-line with information security policy, while providing audit data to verify policy compliance. Also considered is the requirement for an automated analysis tool to quantify the implications of information security policies enforced on cloud hosted workflows and stored data. Such tools could aid policy-makers form more justifiable and financially beneficial security policy decisions.

Section II discusses the provisioning of public cloud resources for workflow deployment while section III examines the main security challenges of public cloud workflow deployments. Section IV outlines core requirements of solutions needed to meet those security challenges. Section V highlights an automated policy-driven public cloud deployment approach with concluding remarks given in section VI.

II. Provisioning Public Cloud Infrastructure for Workflow Deployment

This section briefly examines the concepts of Service Oriented Architecture (SOA) and workflow within an enterprise. It goes on to discuss the current limitations of internal workflow deployment and how public cloud computing infrastructure can help to remove those limitations.

A. SOA and Workflow

Core processes within an enterprise typically define operational best practice. By orchestrating services offered by its existing applications, an enterprise can create new applications and processes in a flexible, agile and cost-effective way. The concept of SOA is well established, removing the need for monolithic and hard-to-manage applications [10]. Each service can be thought of as a software module, carrying out a specific task or action within the high-level application they are part of. Each service processes input data and passes the result on to the next service(s), thus forming a workflow. Data files are managed within the workflow according to a set of security policies (e.g. access control) which aim to achieve the application’s goal in a secure and efficient manner.

B. Internal Deployment Limitations

Workflows have been used in a broad range of domains including business, education and medicine. They typically automate complex and routine processes that are data intensive or computationally demanding. An orchestrator controls the sequencing of tasks, often automatically, and invokes the appropriate enterprise service(s) required for a workflow’s successful completion. Invoked services can be deployed across a set of processing platforms so that performance can be scaled-up to meet demand. However, the availability of internal processing resources can be limited. Unpredictable levels of demand can result in degraded performance levels, underutilisation and increasing costs. This problem is exacerbated by ever increasing productivity needs and data volumes. Through virtualisation and resource sharing an enterprise can form an internal or private cloud which offers some benefits of public cloud computing but still requires a high degree of self-management and can be expensive to run.

C. Public Cloud Infrastructure

Cloud computing naturally extends SOA-based applications out to cloud-delivered processing platforms and storage services. In turn, public cloud infrastructure can offer substantial performance and cost benefits to an enterprise. Enterprises can utilise virtualised and seemingly unlimited on-demand processing hardware for workflow execution and data storage to achieve the necessary performance requirements imposed [6, pp. 7-22].

Significant cost is often invested by an enterprise to provide its current suite of well tested workflows and services. Enterprises do not want the cost and effort of acquiring alternative cloud-based services which may not offer the exact functionality or integration required; may not be reliable or always available; and may be locked in with the cloud vendor [2]. Furthermore, a lack of cloud standardisation means publication and discovery of services in public clouds is not easy [11].

Enterprises need a way to continue running the workflows and services they have in a way that meets productivity and performance needs but without the associated costs. Public cloud infrastructure can offer the required workflow processing environment; the question remains whether that environment is secure?

III. Challenges of Public Cloud Workflow Deployment

Recent surveys (e.g. [1], [3], [8]) suggest that despite its benefits, public cloud adoption within enterprise is being slowed by associated information security risks and compliance issues. A number of works detail these concerns, notably [4], [5] and [9], however no works are apparent that define the security challenges of public cloud deployed
workflows. This section examines the primary challenges currently being faced by enterprises when provisioning public cloud resources and deploying workflows.

A. Lack of Control

Enterprises routinely form data governance strategies comprising of physical controls (e.g. firewalls), transparency mechanisms (e.g. audit logs), and information security policies. Deploying workflows, services and data to public clouds makes the need for governance ever greater as overlooked legal requirements and uncontrolled usage can put an enterprise at risk. The importance of governance is highlighted in [7] with guidance in a cloud setting now starting to emerge.

As no complex configuration is required, workflow deployment and execution on public clouds is becoming easier, thus causing potential security problems. Public cloud suppliers are targeting department managers and end-users, offering infrastructure that can be used within minutes following the provision of a few credit card details [13]. This often occurs without the knowledge or permission of IT and security departments. As many as 50% of CIOs have lost track of cloud computing use within their enterprise, undermining their ability to guarantee the security and compliance of cloud enacted workflows [1]. Furthermore, it is unlikely that departments or end-users wanting rapid deployment assess a public cloud’s security controls with anywhere near the necessary detail, if at all.

Information security policy must encompass applicable data compliance regulations and bespoke workflow security requirements providing a financially justifiable balance between productivity and security [12]. However, the security policies of many enterprises are insufficient when it comes to workflows run in public clouds [3]. The setting of security policies to data files and workflows is time consuming, complex and error prone especially if there is unfamiliarity or lack of concern with information security issues (e.g. inadequate cloud security training [1]). This often leads to inconsistently applied workflow security [6, pp. 76].

B. Workflow Compliance

With no standard for cloud security yet in place, public cloud providers can differ in security control provision making compliant workflow execution assurances difficult. This situation is more challenging as workflow security management typically moves under the control of the public cloud provider.

Enterprises running workflows may have many regulatory mandates to contend with, such as PCI, HIPAA and Sarbanes-Oxley which state how data must be processed, stored and secured. Some of these regulations do not yet consider public cloud deployed data, workflows and services making cloud security (e.g. location, multi-tenancy and data privacy) essential concerns to maintain compliance. Despite this, only 23% of enterprises are requesting proof of current regulation compliance from a cloud vendor [1]. Choosing a cloud provider is often done in an ad-hoc manner with 65% of enterprises evaluating a cloud vendor by word of mouth and only 55% forming bespoke contractual agreements [1]. These contracts may be poorly defined and not offer adequate protection to the enterprise [2]. Furthermore, once a particular cloud infrastructure is adopted, a lack of transparency makes runtime control monitoring and auditing of a cloud’s compliance hard to achieve.

C. Performance vs. Risk

Cloud computing typically comes in three deployment models; public, private or hybrid [6, pp. 22-26]. Much debate and comparison has begun over the benefits of these models in an enterprise setting.

Public cloud hosting is becoming plentiful and may be set up and utilised in moments through a common Web browser. On the one hand, public clouds offer substantial performance benefits while on the other, exposing workflows to potential risk. The limitations of using public clouds in enterprise are discussed further in [2]. An enterprise may choose to rely on its own internal systems and resources configured as a bespoke private cloud. Internal environments are typically comprised of limited resources managed by the owning enterprise yet providing enhanced security with greater control of data.

A hybrid deployment can realise the collective benefits of using both internal resources and those in a public cloud. With information security being a primary concern a hybrid solution offers the enterprise flexibility in choosing combinations of workflow execution environments. Direct control may be maintained over data that is not suitable to move outside the enterprise while data deemed as non-sensitive can be deployed in a public setting. Hybrid solutions would appear to be the approach of choice but leaves enterprises with the problem of deciding where to store data and execute workflows in a dynamic and secure manner.

It is clear that decisions regarding the choice of environment to store data and execute workflows can have a significant impact not only on productivity and cost, but also on information security.
D. Variations to Workflow Runtime Security Requirements

Workflows can often be dynamic in nature due to changes in business and security requirements or from processing different data files [26]. Each instance of a workflow can have different security requirements dependant on the path taken through the workflow (i.e. the services invoked); and input data and user characteristics, both with varying security requirements. Therefore, the suitability of a public cloud to process one workflow instance may not be suitable for the next. Workflows and their services may themselves be deemed sensitive and not suitable for public cloud consumption, despite processing non-sensitive data.

Workflow deployment is often static, so once deployed, either internally or on a public cloud, all instances of that workflow are carried out on that platform. This practice does not lend itself to the ever changing security demands placed on workflows and associated data. Workflows and data need to be deployed in public clouds in a much more controlled and dynamic way.

IV. ACHIEVING SECURE PUBLIC CLOUD WORKFLOW DEPLOYMENTS

To maintain efficient productivity and achieve competitive advantage, enterprises cannot afford to ignore the benefits of public cloud computing [25]. For cloud computing to be cost effective, enterprises need rapid and dynamic workflow deployment which is secure and compliant with information security policy and legal requirements. Cloud computing can offer this if its usage is policy-driven, transparent and controlled. This section defines the core requirements of possible solutions which are needed to achieve these aims.

A. Retaining Control

The self-provisioning of public cloud resources by departments and end-users needs to be controlled. To ensure productivity and cost efficiency is also realised requires a combination of self-service, automation and information security policy [2]. An enterprise must ensure that all public cloud usage first complies with security policy before workflow instances and data can be placed there. Automated deployment (e.g. [20]) on a public cloud may, for instance, be permitted if that cloud is known to provide certain security controls (e.g. data is stored in the UK); while deployment on an unaudited cloud could be allowed if both workflow and data are deemed non-sensitive. Other factors including end-user security clearance, entity owners (of services and data), location and time should be taken into account before deployment decisions can be made.

B. Setting Policy

Global information security policies need to be made fine-grained to allow for unambiguous and compliant automatic deployment decisions. Current policies may need to be supplemented with cloud specific rules to ensure compliance is upheld. Those setting global policies (e.g. CIOs) require a means to self-author and publish automated policies in an easy and secure manner. The usability issues of security policy authoring interfaces are examined in [17] while [18] goes on to describe the need for a template-based authoring framework. These approaches would provide direct control over policy setting by the policy-makers while avoiding misinterpretation by those who may not be completely familiar with applying policies at the technical level [23].

Situations may arise where departments and end-users want to assign more fine-grained security, performance and cost requirements to a workflow, service or data file. Monitoring and control is needed for assigned security policies to be overridden if the enterprise’s global information security policy is not upheld.

C. Monitoring

Enterprises must validate the correctness of security controls and observance of legal mandates to avoid prosecution. Audit data must be made available to augment an enterprise’s data governance strategy by proving compliance, or used as evidence in cases of non-compliance and data breaches. Audit data can also prove useful to identify instances where user applied policies are overridden, and perhaps pinpoint employees and departments that require training or further information security guidance. Furthermore it could be used to detect security policies that may be lacking and require improvement. Accorsi et al [24] present an approach for the auditing of data flow within workflow models to deliver evidence of compliance.

Improvements to information security policy-making and cloud deployment decisions could result from the analysis of workflow executions. Quantifying the financial implications certain policy constraints have on deploying data and workflows would help policy-makers form more justifiable and financially beneficial security policy decisions. Monitoring and cost estimations of cloud usage and its ROI are discussed in [16] and [22].

D. Runtime Security

Potential runtime changes to workflow security requirements need to be considered, especially when run in a public cloud setting. Workflow and data deployment needs to be policy-driven and dynamic, either on internal IT systems or in a public cloud environment according to information security constraints imposed on each instance. Analysis of workflow security policy compliance is addressed in [14] using Petri net models and reachability graphs while [15] offers an approach to verify workflow constraints on information flow in accordance with multilevel security policies. The dynamic deployment of security policies to workflows is examined in [21] while policy-driven cloud resource provisioning has been implemented in [19]. Only if
security requirements are fully satisfied should performance and financial concerns be considered.

V. A DYNAMIC DEPLOYMENT APPROACH

To encapsulate the core requirements for achieving secure public cloud workflow deployments we propose to develop an automated, policy-driven approach that decides where to run workflow instances and store data. Our approach will augment existing workflow management systems with a set of tools concerned with assessing workflow security obligations, workflow instance deployment, runtime audit data, and security policy assignment and analysis. The key responsibility of our approach will be to provide an access control layer in situations where users attempt to provision public cloud infrastructure when executing workflows. The challenge remains to automatically apply the right level of security each time a workflow is run. The main elements of our approach will be as follows:

A. Security Assessment

The security obligations of a workflow instance will be identified through assessing its composition of enterprise services, data files and user characteristics. Each entity would likely be assigned a security classification or policy (by its owner) allowing a security profile of the entire workflow instance to be formed. Enterprise services would need to be assigned a security classification as they may be deemed sensitive even when handling non-sensitive data (e.g. proprietary algorithms). Many of the intermediate data files the workflow instance will handle do not exist before execution, yet their security requirements must be determined. This will be achievable by establishing the workflow instance’s path so identifying which workflow services will be invoked and what data these services will create. Security classification can then be assigned to that data in accordance with an enterprise’s security policy (e.g. ‘output data will have same security classification as the outputting service’) or service algorithm (e.g. ‘all outputs are sensitive’, or ‘output data is sensitive only when input is sensitive’). Further characteristics such as location, time, and the invoking user’s security clearance and privileges would also be considered in line with the enterprise’s security policy.

B. Workflow Deployment

Once a security profile of the workflow has been formed a secured decision mechanism will process workflow execution requests and compare them against the information security policy. A deployment decision can then be formed and the workflow instance’s services and data sent to their permitted processing and storage platforms by an internal, centralised deployment engine. Situations may arise when user specific security, performance and cost requirements are applied to a workflow instance. The decision engine would process such policies and override them if the enterprise’s global information security policy is not upheld.

Deployment presents two potential scenarios; (i) the entire workflow instance executes on a single compliant platform dependant on its most sensitive state (i.e. ‘if sensitive data is present at some point then run internally’) or (ii) sections of the workflow instance are enacting across different processing platforms in a hybrid manner (i.e. ‘sensitive parts run internally’, ‘non-sensitive parts run in public cloud’). Further security policies relating to the invoking user will be considered (e.g. ‘a manager can deploy sensitive data to a public cloud’, whereas an employee cannot). When a public cloud deployment is permitted our approach would aim to choose from a set of audited candidate clouds, taking into account further security policy requirements (e.g. cloud location, multi-tenancy controls), cost requirements (e.g. data transmission, storage) and performance constraints (e.g. advertised uptime, processing speed).

C. Policy Assignment

Global information security policies need to be fine-grained and comprehensive to allow for unambiguous and compliant automatic deployment decisions. Current enterprise information security policies should be supplemented with cloud specific rules where needed. These additional rules will manage public cloud scenarios to ensure compliance continues with existing policy and legal mandates (e.g. Data Protection Act 1998), including where services and data can be deployed (e.g. ‘internal only’, ‘UK based cloud’, ‘public cloud if data is encrypted’, etc.); which audited public clouds can be used (e.g. location, multi-tenancy provisions, guaranteed uptime, etc.); and user privileges stating who can deploy what, when and where to public clouds (e.g. ‘a manager can deploy encrypted sensitive data to a UK based cloud from their own office PC between 9am and 5pm’). Those applying policies (e.g. CIOs) will be provided with a means to author and update policies in an efficient and complete manner resulting in policies that must be automated via a suitable policy language and stored in a secure repository.

D. Audit Data

For compliance purposes, a mechanism is required to monitor and log all aspects of the decision making and deployment process. This will provide audit data to clarify policies are comprehensive, correctly constructed and applied; data and services are classified correctly; and deployment activities achieve compliance. Data would also be available to identify end-user behaviour and pin-point where cloud security training is needed (e.g. users consistently attempting execution of sensitive workflows in a public cloud environment).
E. Policy Analysis

As part of our approach an automated tool would use the audit data and available cost information to quantify the financial implications particular policy constraints have on deploying workflow instances and data to different execution environments. Cost information would include both operational costs (e.g. storage and infrastructure rates) and performance costs (e.g. deployment and execution time). This analysis data would be useful to security policy-makers to help them make more informed and cost effective policy decisions. For example, risk-benefit comparison between a workflow instance executed internally against an imagined performance costs (e.g. deployment and execution time).

This section describes how this automated tool could help policy-makers form more justifiable and financially beneficial security policy decisions. Future work sees the development of our approach.

VI. CONCLUSION

Public cloud computing is beginning to emerge as a new environment for workflow enactment. The scientific community is yet to define the security issues of deploying workflow instances to a public cloud setting and articulate solutions to ensure deployment is compliant with enterprise policy and legal mandates. This paper has begun to address this shortfall by highlighting the prevalent information security issues being experienced by enterprises currently using public cloud infrastructure. Workflow instances and data are being deployed to public clouds in a potentially unsecured and uncontrolled manner. Information security policies and training are inadequate when it comes to public cloud use, and many employees are ‘self-serving’ cloud resources, without the permission of senior management. A major issue is that the security requirements of a workflow can vary with changing business needs and the processing of different data files, meaning a single static execution environment is not always suitable for every instance. The paper has also defined the core requirements for solutions to provide compliant yet rapid and dynamic workflow deployment.

Enterprises require a combination of self-service, automation and information security policy. We have proposed an automated dynamic and policy-driven approach is needed to choose where to run workflow instances and store data while providing audit data to verify policy compliance and avoid prosecution. Also suggested is an automated tool to quantify information security policy implications to help policy-makers form more justifiable and financially beneficial security policy decisions. Future work sees the development of our approach.

REFERENCES