ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Survey On Information Flow Control for Secure Cloud Computing

Priyanka S. Mane, Yogesh B. Gurav

ME Student, Dept. of Computer Engineering, Padmabhooshan Vasantdada Patil Institute of Technology. Savitribai Phule Pune University, Maharashtra,India.

Professor, Dept. of Computer Engineering,, admabhooshan Vasantdada Patil Institute of Technology. Savitribai Phule Pune University, Maharashtra,India.

ABSTRACT: In today's field of technology, the popularity of cloud computing is increased due to its high potential to provide fast computing services over the internet. So security aspect is important consideration in cloud computing. It is examined that there is less assurance about security in cloud services. Information Flow Control (IFC) is a Mandatory Access Control method, a genuine apporach for access control management of data with ample security. The initial IFC models provide security for centralized domains; but now a days IFC models for decentralized database has been developed by many reserachers. Respectively , decentralized IFC have a good potential to gain secure cloud services compared to other models working today. In this paper we study and review a range of IFC models and approaches to identify opportunities for using IFC within a cloud computing context. Since IFC security linked to the data that it protects, both tenants and providers of cloud services can agree on security policy, in a manner that does not require them to understand and rely on the particulars of the cloud software stack in order to effect enforcement.

KEYWORDS: Decentralized information flow control, information flow control, access control, secure cloud computing, data security, labelling.

I.INTRODUCTION

Now-a-days cloud computing is emerging technology provides practical, inexpensive, on-demand access to resources. It is *utility computing*—the vision of the Grid and other distributed systems before it. Although cloud computing is depend on a collection of research areas like, distributed and grid computing [3], [4] service-oriented-architecture (SOA) [5] and virtualization [6], [7], this technology now become a promising computing paradigm captures tremendous attraction from both industry and academia. It has shown extensive capability to increase availability, scale, agility and collaboration.One of the unsatisfactory thing about cloud computing is the lack of security assurance. Unless cloud users/tenants trust cloud providers, use of cloud computing solutions will decreased. The security issue in cloud computing is challenging because of its wide range of technical and legal aspects. Data leakage concern of cloud computing is holding back more widespread promotion of cloud computing by industries, public institutions and academics alike. There is an increasing extent of ratification [8], but fortifying and signifying compliance with the ratification by cloud service providers and third parties is controversial. In recent work, we have explored the work of Information Flow Control (IFC) for distributed cloud computing. We made a proof-of-concept execution of the quality IFC model as a basis for estimation [9]. By this experience, we assume that the disposition of IFC to expand traditional authentication and authorization has the prospective to make a significant contribution for security of distributed and cloud systems, with both enforcement mechanisms and demonstration of acceptance by audit. Nevertheless, the utilization of IFC for large-scale data analytics is complicated using the standard IFC model.

In this paper, we present a survey on augmented IFC model, which, while preserving the clarity of expression and execution of the standard model, easily expands to large scale. Much work remnant to completed, especially when cloud services integrated as part of wide-scale distributed systems, as in Internet of Things (IoT) [10]. In a cloud infrastructure, if IFC integrated into cloud service as part of SaaS or PaaS clouds, it can yield continuous, data-centric access control policy across and within applications. This survey paper focuses on access control issues in cloud computing environments. Paper focus is toward the issues, which would raise significant concerns from customers,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

which can be of organizations or enterprises when they outsource data and individuals. Vulnerable information flows [11] exist in clouds at a high amount since a service provider can access number of cloud virtual machines where multiple customers' data are stored. This can elevate conflict-of-interest challenges when the service provider reveals sensitive information of usersto other rival customers for commercial gain, which can cause massive loss to a customer. This issue is clearer when concern services are roaming into clouds. It is natural that consultants have to tackle with confidential data stored in clouds for their users. In this paper, we reviewed some previous technologies based on information flow control mechanism with their advantages and disadvantages details in next section.

II.RELATED WORK

This survey articulate previous methods of information flow control mechanisms, let see their details. Here in this section we are going to give brief overview of previous IFC based techniques. With detailed introduction, we would mention advantages, drawbacks and future enhancements of respective techniques. Let see this methods in detail in following discussion.

1. FlowK [12]

Paper depicts how, FlowK can be integrated with cloud software. We have designed and evaluated a framework for deploying IFC-aware web applications, suitable for use in a PaaS cloud. Our design based on "policy-mechanism separation", in that the enforcement of IFC in FlowK separated from any knowledge of principals, users and the management of privileges. This separation ensures maximum flexibility for higher levels of software; this work contributes: (1) without modifying monitored access of standard OS it includes IFC within it like other systems. (2) To achieve requirements for isolated processing it supports conflicts of interests in IFC model. (3). It depicts how FlowK intergrated with applications to create framework for PaaS-cloud. Idea of FlowK is based on decentralized IFC model (DIFC) introduced in 1997. Decentralized model has been outlined for varying needs like static, global, hierarchical levels of security to fluid systems and capable of satisfy this needs of different applications. In this, model every entity having two labels: integrity label and secrecy to catch confidentiality/privacy and reliability of source data, these labels have security tags.

By above description we can conclude that FlowK does not require any changes to system calls so unmonitored processes not affected by the existence of FlowK as an OS module, apart from a small performance overhead. The security context manipulation done through a small, well defined set of API calls. The FlowK kernel module is concerned only with enforcement of IFC, following policy-mechanism separation. In FlowK we have a straightforward and efficient starting point for IFC enforcement in cloud computing. Regarding this concept, In future, we will explore application policies in more detail and their enforcement via IFC. We are integrating FlowK with an IFC enabled messaging middleware (SBUS-IFC) to create more general application structures for distributed and cloud computing

2. Integrating Messaging Middleware and Information flow control [13]

To secure data flows within virtual machine author proposed kernel level protection by applying IFC enabled middleware. Paper describes IFC enables messaging middleware. This approach decides IFC constraints on each data flow within virtual machine. This messaging middleware approach apply IFC across systems which secures data travelling between services (storage) and applications, which is local to virtual machine. To achieve this author introduced concept SBUS middleware enabled by IFC (i.e. SBUS-IFC).SBUS-IFC messaging middleware strongly supports range of communication paradigm- broadcasts, stream based and request-reply; typed messages, security like encryption and access control. Dynamic reconfiguration supported by SBUS mainly, where it provides facility for third parties to manage application's communication as application itself, which add simplification at deployment and development to application. Here for SBUS, component is main process, which belongs to application for managing communication and supports hierarchical message structure (i.e. attribute can contain number of sub attributes). So here author mainly emphasis on two things: (1) Describes efficiency of integrated IFC enabled middleware carry in cloud context. (2).Related performance overhead measured.

We can draw conclusion that in this paper, IFC enabled middleware shown practically. This work describes IFC control in services, containers, virtual machines, providers, for users, across applications. Proposed mechanism able to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

separate services and applications from their code, which helps to preserves security in cloud. Author successfully integrated IFC middleware with local mechanism (FlowK) provides protection across applications.In this paper aim was to maintain end-to-end information flow control but assignment of global unique names to tags of application not considered here which will include in future frameworks. Here IFC considers channels and bytes so there is need to extend this work for fine-grained IFC policy. In future, we can apply IFC mechanism to 'Internet of Things'.

3. Information Flow Control for Cloud Computing [14].

In this paper, we propose an approach to enforce the informationflow policies at Infrastructure-as-a-Service (IaaS) layerin a cloud-computing environment. Especially, we adopt Chinesewall policies to address the problems of insecure informationflow. We implement a proof-of-concept prototype system based on Eucalyptus open source packages to show the feasibility of our approach. This system facilitates the cloud management modules to resolve the conflict-of-interest issues for service providers in clouds. Several key challenges need to address like Selection of Appropriate Service Layer and Definitions for Policy Components.

we can conclude that author first identified the information flow problem, which could raise conflict-of-interest issues in cloud computing environments. In addition, we have articulated challenges in specifying and enforcing information control policies in cloud computing. To address the identified problem and challenges, we proposed an approach to enforce the Chinese wall security policy at the laaS layer of a cloud. We also implemented a prototype system based on Eucalyptus open-source software to prove the feasibility of our approach.In future for instance, we would investigate how laaS management can be complied with both PaaS and SaaS. In addition, a user may wish to delegate his cloud instance access privileges to others. A practical delegation mechanism is another essential component for cloud computing.

4. Silver Lining: Enforcing Secure Information Flow at the Cloud Edge [15].

In this paper author, proposed policies for Java computations on commodity, data processing, platform –as-a-service cloud by Aspect-Oriented programming (AOP) and In-Lined Reference Monitoring (IRMS).This method provide in-lines secure information flow tracking code into un-trusted Java job binaries in cloud. This facilitates efficient enforcement of large and mandatory access policies without any customize cloud. Silver Lining makes no changes to the cloud infrastructure, which is fully transparent to Java job author with no changes to Java bytecode or API. Result shows the efficiency and scalability of silverLine with low overhead. This technique adds mandatory access control policies as well as secured information flow policies for Hadoop clouds on non-trustworthy java job binaries [16] but execution is completely distinct to rest cloud. Information flow graph (IFG) maintains distributed data resources within loud and tracks information flow. In-lined Reference Monitor restricts non-secured information flow at cloud edge. Aspect oriented programming [17] helps to in-line and implement IRMs into un-trusted jobs without any interfere to job source codes. Execution carried on synthetic jobs and real world jobs that sliverLine not require any change in existing binaries and work seamlessly.

After detailed observation, we can conclude that, SliverLIne is first development based on Hadoop cloud information flow, which does not require any changes in cloud infrastructure. In addition, this is solely apparent for java users, which does not require any change in java byte code or API. The work proposed in this paper based only on mandatory access control policies of information flow between resources. SliverLine Efficiency and scalability achieved through low overhead. Verification algorithms used here are smaller than the code-rewriting environment so more trustworthy.In future workflow computations would expressed in other languages such as native code, which is wholesome platform for such extension. There is scope to extend security policy languages and classes on larger and expensive manner. We can investigate feasibility of verification algorithms to endorse IRMs in cloud.

5. Information flow control for strong protection with flexible sharing in PaaS [18]

This is data-centric method. Paper depicts how information flow control, mechanism is suitable approach for data centric environment. IFC based cloud platforms are able to provide fine-grained control while data sharing. Idea behind IFC is to control information leakage while data exchange. In this paper author proposed, model which tender with common IFC assurance (i.e no write down, no read up [17]) and no integrity (no write up, no read down [18]).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

IFC have security tags named as token, which mentions security concerns, each entity like messages, application instances, sockets and any data exchange platform having this tags. Each entity assigned two labels: secrecy label and integrity label. Linux kernel module used for execution for an IFC based web service framework. IFC based messaging middleware integrated with FlowK.

In this paper author contributed isolation approach to manage data sharing. This technique introduces mechanisms as structured messages having individual label for attributes for middleware integration. Here we aimed to maintain maximum transparency for IFC.In future IFC mechanism can implemented in various levels in cloud stack, like the one-structured objects of policy operate at higher level than operating system. IFC can be enforcing to execute at end-to-end, and possible to apply global naming scheme to tags.

6. A distributed access control architecture for cloud computing [19]

This paper focusing on fulfilling access control needs of cloud users. Author presented distributed access control architecture based on ethics of security and software engineering for virtualized environments and multitenant. In distributed cloud, side-channel attacks and interference among different policy domains are main challenges. Author tried to overcome these challenges. Vertical and horizontal policies for service delivery allowed in cloud to support decentralized environment. Proposed architecture having three components: (1) Distributed access control (ACM), (2) Service level agreement (SLA), (3) Virtual Resource Manager (VRM). This architecture based on RBAC model for simplified administration and scalability. VRM is for deploying and providing virtual resources and maintains granularity and heterogeneity virtual resources in cloud. ACM is responsible for applying access control policies at resident layer. Main components of ACM are policy base, policy enforcement point, policy decision point. Authorization request transferred to Policy Enforcement Point, which contains requested resources/ services, requested subject and permissions for those resources. PEP then extracts required credentials from that request and forward to context evaluator and credential evaluator. PEP accepts granting request decision and decides whether to accept or denies users authorization request. SLA performs billing and auditing of functions, role mapping, prevent side channel attacks and pose virtualized view of resources. SLA isolates resources to secure side channel attacks for remote cloud, which helps to restrict multiple VMs to reside on same physical machine. Physical isolation enforced according to rule of RBAC policy by setting cardinality constraints. RBAC policy based on XML specification of SLAs and ACMs, which help to achieve goal that proposed system should be interoperable with security protocols for cloud infrastructure. In this paper author proposed architecture for distributed cloud environment. Problems of side channel attack and interference among different policy domains have solved.

7. FlowR[20]

This paper focused on information flow control mechanism based on aspect-oriented programming. Main idea behind paper work was to sustain the use of unchanged platform as service (PaaS) cloud environment through IFC based web applications. Here Thomas and Jean Bacon mentioned how aspect oriented programming helps to overcome drawbacks of RubyTrack. Ruby enhanced to provide IFC primitives through aspect oriented programming by using aquarium open source library. FlowR able to isolate functional execution and security concerns which results in easier maintenance and development. Author focused on problems are: (1) first author assumed that developer is not foe; aim is to preserve against discloser of information by foe through bugs or errors in application. (2) Focusing on structure of web application by using different frameworks like Rails to be or Sinatra for example established on Platform as a Service cloud by using available interpreters. (3) Preserve data privacy. Last author assumed that applications executed by organizations are ready to receive information exchange for incremental security promise.Aspect oriented security is a programming approach which enhance object oriented paradigm by enabling cross cutting aspects. Aspect means piece of code named as advice in combination with pointcut. The pointcut used to determine objects methods where, advice would implement. An advice implemented before or after joint-point execution. In FlowR IFC Model DEFCon project [12] extended by applying IFC to objects, methods and classes. Here author proposed model for single application instead of multi application environment.Flow control and tracking mechanism provided on arbitrary objects, methods, classes and basic variables like integers, strings, floats. Each object tracked by two labels[2]: send label and receive label are security labels. Receive label depicts type of information which flow in object and send label shows behavior and sensitivity of objects.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Through this paper study, we can draw conclusion that approach mentioned in this paper is nice solution to apply IFC when there is not any application running. This approach is not limited to ruby but can depict for any OO language, which support AOP. This mechanism requires less maintenance and more innovative provides great security and performance. Library does not require code rewriting so not require any change in program behavior. In this paper application functionality separated from security concerns. There are issues like, it does not support multithreading and when number of AOP advice executed on same object. In future, aspect oriented programming used for information flow control having various advantages, which extend in future based cloud context.

8. Information Flow Control forSecure Cloud Computing[1]

In this paper the author describes the properties of cloud computing Platform-as-a-Service clouds in particular and review a range of IFC models and implementations to identify opportunities forusing IFC within a cloud computing context. Since IFC security is linked to the data that it protects, both tenants and provider sof cloud services can agree on security policy, in a manner that does not require them to understand and rely on the particulars
of the cloud software stack in order to effect enforcement.

The author argue that data-centric security mechanisms such as Decentralised Information Flow Control (DIFC) have the potential to enhance today's cloud security approaches. It envision future secure cloud computing platforms that support the attachment of security policies to data and use these policies at runtime to control where user data flows.Such data-centric security mechanisms, which track oren force information flow, can improve cloud security in many ways. First, developers are given the ability to coordinate with the cloud provider and control how user data propagates ina cloud platform. This facilitates compliance with regulatory frameworks. Second, multi-tenancy, i.e. the practice of sharing services between cloud tenants, becomes more secure because the cloud platform can impose checks to enforce security policies[2]despite flaws in the services themselves. Third, tracking data flows across different services offers the cloud provider away to log sensitive operations on tenant data rigorously, thus improving accountability.In this paper the author investigate the feasibility of deploying IFCas part of the next generation of secure cloud infrastructures. It review research on information flow tracking and enforcement and evaluate data-centric security models. The contribution is to show that despite the open challenges that remain to be addressed, IFC models and implementations can lead to practical and more secure cloud computing infrastructures.

From above discussion we can conclude that DIFC is most appropriately integrated into a PaaS cloud model. DIFC has been used to protect user data integrity and secrecy. A number of challenges need to be overcome. These include: selecting the most appropriate DIFC model; policy specification, translation, and enforcement; audit logging to demonstrate compliance with legislation and for digital forensics. DIFC should not impose an unacceptable performance overhead and it is important that application developers using cloud-provided IFC are aware of the trust assumptions inherent in the IFC provision. We plan to address these challenges in our future work.

III.MERITS AND DEMERITS OF DIFFERENT APPROACHESOF IFC

After reviewing different techniques of Information Flow Control the pros and cons are tabulated.

IFC models	Mechanism	Merits	Demerits
FlowK	It enforce information flow control with "policy-mechanism separation".	• It gives maximum flexibility. • It supports conflict-of-interests in IFC. • Small performance overhead.	• Low performance. • Application policies are not taken into consideration.
Integrating Messaging Middleware and Information flow control	It enforce IFC by messaging middleware approach. This approach decides IFC constraints on each data flow within	• It provides high security and supports dynamic reconfiguration. • Good efficiency and end –to-end information	• Does not support global unique names to tags of application. • It does not provide fine-grained IFC policy.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

	virtual machine.	flow control.	
Information Flow Control for Cloud Computing	It adopts Chinese wall security policy for information flow control at IaaS layer in cloud.	• It ensures feasibility. • It facilitates the cloud management modules to resolve the conflict of interest issues for service providers in cloud.	• It consider IaaS cloud service layer and not complied with PaaS and SaaS cloud. • It lacks in proving practically.
Silver Lining: Enforcing Secure Information Flow at the Cloud Edge	It defines policies for JAVA computations on commodity, data processing, PaaS service cloud by Aspect-Oriented programmingand In-Lined Refernce Monitoring.	• It facilitates efficient enforcement of large and mandatory access policies. • It gives good efficiency and scalability. • It makes no changes the cloud infrastructure. • Low performance overhead.	• Low performance. • It is solely apparent for JAVA users.
Information flow control for strong protection with flexible sharing in PaaS	It uses data-centric method. It depicts how information flow control mechanism is suitable approach for data centric environment.	• It gives maximum transparency. • It provides fine-grained control while data sharing.	• It lacks in integrity. • Does not enforce end-to end IFC.
A distributed access control architecture for cloud computing	It defines a distributed access control architecture for virtualized environments and multitenant.	• resolves problems of side channel attack and interference. • Provides scalability • It maintains granularity.	• The focus is limited to virtualized environment. • Restriction on number of virtual machines on same physical machine.
FlowR	Information flow control mechanism based on aspect-oriented programming. Provides IFC for PaaS cloud.	• Provides great security and performance. • Less maintenance.suitable for any object oriented language.	• It does not support multithreading and when number of AOP advice executed on same object.
Information Flow Control for Secure Cloud Computing	Decentralised Information Flow Control as data-centric security mechanism.	• Provides high security and feasibility. • Provides data integrity. • Compatible for all three cloud IaaS, PaaS & SaaS service layers.	• Lack in trust assumptions. • Unacceptable performance overhead.

IV. CONCLUSION AND FUTURE WORK

In this paper, we reviewed various techniques based on IFC, for cloud infrastructure. We observed working of those techniques and tried to find out there pros and cons. In addition, we mentioned what kinds of future enhancements are possible in respective techniques. This survey will definitely help the researchers to set their own goals for decentralized information flow control according to specific demands.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

REFERENCES

[1]Jean Bacon, David Eyers, Thomas F. J.-M. Pasquier, Jatinder Singh, Ioannis Papagiannis, and Peter Pietzuch, Information Flow Control for Secure Cloud Computing, IEEE Transactions On Network And Service Management, Vol. 11, No. 1, March 2014.
[2]David Schultz, Barbara Liskov, IFDB: Decentralized Information Flow Control for Databases, ACM , Eurosys'13 April 15–17, 2013.
[3] l. Foster, C. Kesselman, J. Nick, and S. Tuecke. The physiology of the grid: An open grid services architecture for distributed systems integration. In Open Grid Service infrastructure WG, Global Grid Forum, volume 22, pages 1-5. Edinburgh, 2002.
[4] l. Foster, Y. Zhao, l. Raicu, and S. Lu. Cloud computing and grid computing 360-degree compared. ArXiv e-prints, 901:131, 2008.
[5] T. Ert. Service-oriented architecture: concepts, technology, and design. Prentice Hall PTR Upper Saddle River, NJ, USA, 2005.
[6]P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield. Xen and the art of virtualization. In Proceedings of the nineteenth ACM sympOSium on Operating systems principles, page 177. ACM, 2003.
[7] M. Vouk. Cloud computing Issues, research and implementations. In 30th International Conference on Information Technology Intel!aces, 2008. ITI 2008, pages 31-40, 2008.
[8] C. J. Millard, Ed., Cloud Computing Law. OUP, 2013.
[9] T. F. J.-M. Pasquier, J. Bacon, and D. Eyers, "FlowK: Information Flow Control for the Cloud," in 6th International Conference on Cloud Computing Technology and Science (CloudCom). IEEE, Dec 2014.
[10] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "20 Cloud Security Considerations for Supporting the Internet of Things," under review.
[11] J. McLean. Security models and information flow. 1990.
[12] Thomas F. J.-M. Pasquier, Jean Bacon, David Eyers, "FlowK: Information Flow Control for the Cloud"
[13] Jatinder Singh, Thomas F. J.-M. Pasquier, Jean Bacon, "Integrating Messaging Middleware and Information Control", IEEE , 2015
[14] Ruoyu Wu, Gail-Joon Ahn, Hongxin Hu, Mukesh Singhal, " Information Flow Control For Cloud Computing", IEEEConference publications , 2010.
[15] Safwan Mahmud Khan, Kevin W. Hamlen, Murat Kantarcioglu, "Silver Lining: Enforcing Secure Information Flow at the Cloud Edge" , IEEE, march 2014, pp. 37-46.
[16]"ApacheHadoop",http://hadoop.apache.org,2013.
[17]G. Kiczales, J. Lamping, AMendhekar, C. Maeda, C. Lopes, J.-M Loingtier, and J. Irwin, "Aspect- oriented programming", in proc. European Conf. object oriented programming(ECOOP), 1997, pp. 220-242.
[18] Thomas F. J.-M. Pasquier, Jatinder Singh, Jean Bacon, "Information flow control for strong protection with flexible sharing in Paas", IEEE, 2015.
[19] Abdulrahaman A.Almutairi and Muhammad I. Sarfraz, saleh Basalamah, walid g. Aref Ghafoor, "A distributed access control architecture for cloud computing " ,IEEE, 2012, pp. 36-44.
[20] Thomas F. J.-M. Pasquier, J Bacon, " FlowR: Aspect Oriented Programming for Information Flow Control In Ruby", IEEE, 2014, pp. 37-47