Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 52 (2015) 318 – 325

Procedia Computer Science

The 6th International Conference on Ambient Systems, Networks and Technologies (ANT 2015)

Towards the Certification of Covert Channel Freeness in Cloud-Based Systems

Jason Jaskolka*, Ridha Khedri

Department of Computing and Software, Faculty of Engineering, McMaster University, Hamilton, Ontario, Canada

Abstract

The rapid transition to cloud-based infrastructures has introduced a number of uncharted risks, threats, and challenges that are faced by security experts. In particular, concerns surrounding the confidentiality of information in cloud-based systems and the existence of covert communication channels ought to be addressed.

In this paper, we outline a schema for certifying covert channel freeness in cloud-based systems. The proposed schema provides an application of the formal foundation laid out in our previous work and is based on a strategy derived from the necessity and formal verification of the conditions for covert channel existence in cloud-based systems specified using the mathematical framework of Communicating Concurrent Kleene Algebra (C^2KA). We also discuss how the proposed schema can be used for identifying ways in which an analyst may amend, modify, or redesign a system in order to make it more resilient to covert channels, and to potentially certify it to be free from covert channels on the basis of the non-existence of the potential for communication amongst its agents.

Peer-review under responsibility of the Conference Program Chairs

Keywords: covert channels, cloud computing, security, confidentiality, certification

1. Introduction and Motivation

The emergence of cloud-based computing has substantially altered the perception of infrastructure architectures and models for software storage and development. It has quickly gained popularity and has enjoyed a recent thrust into the mainstream. However, as the push for cloud-based computing surges, so do the concerns regarding the security and particularly, the confidentiality of information in cloud-based systems. The rapid transition to cloud-based infrastructures has fuelled a number of uncharted risks, threats, and challenges that are faced by security experts [1].

Cloud computing is an umbrella term that refers to a category of computing services, such as storage and software, and denotes a model where an infrastructure is viewed as a "cloud" from which agents can access applications from anywhere in the world on demand [2]. Such an infrastructure has been offered by commercial providers, such as Amazon, Google, and Microsoft.

Cloud-based systems are specific kinds of distributed systems of communicating agents. A *system of communicating agents* refers to any collection of interacting agents. Throughout this paper, the term agent shall be treated in the

* Corresponding author. Tel.: +1-905-525-9140 ; fax: +1-905-524-0340.
E-mail address: jaskolj@mcmaster.ca

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2015.05.100

sense used by Milner[3] where an *agent* refers to any system whose behaviour consists of discrete actions. In this way, an agent may just as easily be perceived as a system process, component, or service, each of which are terms used in the literature of cloud-based computing (e.g., Zissis and Lekkas[1], Buyya et al.[2], Krutz and Vines[4]).

While there exists many concerns surrounding the confidentiality of information in cloud-based systems, one particular concern is that of the establishment and operation of covert channels[5]. A covert channel refers to any communication means that allows an agent to transfer information in a manner that violates a system's security policy[6]. In the literature, covert channels have also been referred to as subliminal channels[7] and steganographic channels[8]. Typically, covert channels are hidden from the view of third party observers. Because of this, the use of covert channels often results in third-party observers not even necessarily being aware that any communication is taking place at all. In this way, covert channels provide a means for data exfiltration, allowing for sensitive information to be leaked secretly to agents for which the information was not intended. Particularly, one can imagine that in a cloud-based system, which may be perceived as a complex infrastructure with many interacting agents, covert channels can be widespread across the entire infrastructure. Furthermore, due to the significant amount of resource sharing upon which cloud-based systems are built, system agents can utilise any number of different communication mediums, channels, and techniques in order to establish covert channels. This is consistent with the perception of covert channel communication given by Jaskolka and Khedri[9].

With such a significant concern surrounding the confidentiality of information in an increasingly popular computing infrastructure, we ought to strive for mechanisms to eliminate or, at the very least, minimise these threats. Because of the scale and complexity of cloud-based systems, the need for a systematic analysis for the existence of covert channels is becoming increasingly important. Currently, cloud-based systems lack assurance of the protection from confidentiality vulnerabilities such as covert channels[1]. Such an assurance needs to be provided at the early stages of the software development life-cycle.

In this paper, we outline a schema for assuring covert channel freeness in cloud-based systems. This assurance comes in the form of a certification. In this context, certification refers to the ability to mathematically substantiate the non-existence of covert channels in a given system. The certification schema outlined in this paper provides an application of the formal foundation laid out in our previous work[10,11,12,13]. Specifically, the proposed schema is based on the specification of cloud-based systems using the mathematical framework of Communicating Concurrent Kleene Algebra[11,12] (C^2KA) and an analysis of the necessary conditions for covert channel existence[10] at an early stage in the development of a system, namely at the system specification stage. Without discussing all of the details of the formal specification of cloud-based systems and the formal verification of the necessary conditions for covert channel existence due to space limitations, we focus on discussing the proposed schema for the certification of covert channel freeness. The process on which the proposed schema is based opts for an approach that aims to falsify the potential for communication condition. We think that the proposed schema for certifying covert channel freeness in cloud-based systems can lay the grounds for having systems which are assured to reduce the concerns surrounding information confidentiality and privacy in the cloud.

The remainder of this paper is organised as follows. Section 2 discusses the existence of covert channels in cloud-based systems. Section 3 presents the necessary conditions for covert channel existence in systems of communicating agents. Section 4 outlines the setting, strategy, and schema for certifying covert channel freeness in cloud-based systems. Section 5 identifies and discusses how the proposed certification schema can guide an analyst to amend, modify, or redesign a system in order to make it more resilient to covert channels, and to potentially certify it to be free from covert channels on the basis of the non-existence of the potential for communication amongst its agents. Finally, Section 6 gives concluding remarks and provides the highlights of our current and future work.

2. Covert Channels in Cloud-Based Systems

In modern computer systems, covert channels are regularly based on obscure and unexpected uses of system resources and functionalities. Covert channels generally arise from resource sharing and the ability to devise covert communication schemes based on some shared knowledge about the system. In order to eliminate covert channels, all contention for shared resources must be minimised and there must be enforceable restrictions on what agents are able to know and communicate.

Cloud computing is based on a model where resources are shared. In particular, a number of agents share the same computing resources at the network level, host level, and application level. Although the agents are virtually isolated

from one another, the hardware is not separated[1]. Both the virtualisation environment and the resource sharing of cloud-based systems allow for fruitful avenues for the establishment of covert communication channels. Many cloud-based systems attempt to maximise efficiency by assigning multiple virtual machines to execute on the same physical server. They also allow for "multi-tenancy" which is the multiplexing of the virtual machines of disjoint agents upon the same physical hardware[14]. Thus, it can be conceived that an agent's virtual machine could be assigned to the same physical server as another, possibly malicious, agent. Furthermore, it is possible that agents can share virtual services which can be used for covert communication. In turn, this provokes the threat that an agent may penetrate the isolation between virtual machines resulting in potential violations of confidentiality. For instance, due to the virtualisation environment of cloud-based systems, they become vulnerable to cache-based covert channels[5] and keystroke activity channels[14]. Additionally, Salaün[15] gave a description of covert channels in the Xen hypervisor virtual machine system which has recently been introduced to cloud-based systems. In particular, these covert channels use the mapping table between physical addresses and pseudo-physical addresses of the hypervisor to write covert information that can be read by other agents in the system.

With the significant amount of resource sharing that is required in cloud-based systems, the potential for timing-based covert channels is dramatically increased. For instance, the constant time interval and varying time interval channels[16], and the marked packet timing channel[9], pose a significant threat due to the number of resources and functionalities that can be utilised as the signalling mechanism. Furthermore, the threat of the existence of timing-based covert channels is particularly evident since many cloud-based systems provide some level of reliability in the form of acknowledgement-based communication (e.g., Mehmood et al.[17]). The potential for agents to alter the timing of acknowledgements affords the ability to employ a wide-range of covert channel constructions in order to leak confidential information in a cloud-based system.

In addition to the above mentioned covert channel threats, the network architecture of cloud-based systems provides another medium for establishing covert channels. Apart from piggybacking on common network protocols which are used in cloud-based systems, such as TCP (e.g., Smeets and Koot[18]), covert channels can be established using bouncing techniques which take advantage of third party equipment, (e.g., an arbitrary number of cloud servers) that can relay information between the source and destination[19].

Although we did not exhaust all of the types of covert channels that can exist in cloud-based systems, we have illustrated that cloud-based systems afford an ability to establish many types of covert channels which can result in the potential for confidential information leakage. For this reason, this paper outlines a schema for reducing such concerns in the form of a certification of covert channel freeness in cloud-based systems.

3. Necessary Conditions for Covert Channel Existence

One of the main challenges and first steps towards safeguarding cloud-based systems against the threat of covert channels is determining the necessary conditions under which a covert channel may exist in a given system. In previous work[10], we articulated a set of necessary conditions for covert channel existence. In a given a system of communicating agents, if there exists a covert channel, then the following conditions are satisfied:

1. *Potential for Communication*: If there exists an agent acting as a source of information and an agent acting as an information sink, such that the source and sink agents are different, and if there exists a pattern of communication allowing for information to transfer from the source to the sink through the synchronisation and sequencing of events, then the source and sink agents have a potential for communication.
2. *Constraint on Communication*: If there exists confidential information in the data store of an agent, then there is a constraint on the communication of the agent and the agent can be a source of information.

The *potential for communication* condition considers the behaviour of the system agents and captures *how* information can be communicated by the agents in the system. It captures the ability to initiate an information flow from a sending agent to a receiving agent. Such information flows may be established through the synchronisation of events in the system via timed events or communication handshakes, for example. This kind of synchronisation of events allows for the creation of a "pattern of communication" or simply a sequence of events that allows information to flow from one agent in the system to another. In essence, as long as there is a potential for information to flow from one agent to another, it is possible for a communication channel to be established and there is a potential for communication in the system.

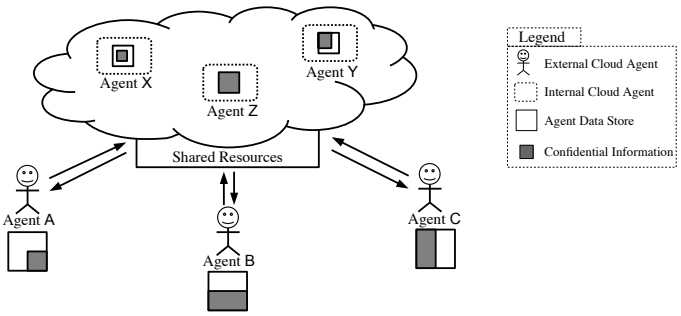

Fig. 1. A cloud-based system with internal and external cloud agents with data stores containing confidential information.

Conversely, the *constraint on communication* condition considers the knowledge of the agents in the system and captures *what* information each agent can know and communicate. In this way, only covert channels affording an ability to violate the security policy employed by the system through the threat of confidential information leakage are considered to be covert channels. This is to say that if an agent does not know any confidential information, then regardless of any potential communication means, covert or otherwise, there is no possibility for that agent to communicate any confidential information to violate the security policy and therefore, under the definition of covert channels adopted in this paper, there is no possibility for the existence of a threatening covert channel with that agent as the source of information. Such an agent can only be an intermediate agent that relays information between a source and a sink.

4. A Schema for Certifying Covert Channel Freeness in Cloud-Based Systems

In what follows, consider a system of communicating agents where each agent has an associated data store. Suppose that there exists a security policy that specifies which information from each agent's data store is permitted to be shared with other agents in the system. In this way, each agent has its own set of confidential information. Furthermore, suppose that the security policy explicitly forbids the communication of the confidential information of any particular agent to any other agent. Under this setting, we can equate this kind of system of communicating agents to a cloud-based system where there may be a number of cloud agents, each with their own local data store and set of confidential information that should not be leaked to any other agent. Additionally, it is important to note that each cloud agent can have information which is permitted to be communicated and shared with the other agents in the system. It should be noted that a cloud agent may refer to both a client (external cloud agent) in the cloud-based system, as well as any component, process, or service, (internal cloud agent) provided by the cloud itself. This setting is illustrated in Figure 1.

4.1. A Strategy for Certifying Covert Channel Freeness

Assuming the setting outlined above, we outline the strategy that is taken towards the development of a schema for certifying covert channel freeness in cloud-based systems. The general strategy for establishing a schema for certifying covert channel freeness in cloud-based systems is a consequence of the necessity of the conditions for covert channel existence presented in Section 3. This is to say that, if a covert channel exists in a given system of communicating agents (e.g., a cloud-based system), then the potential for communication condition and the constraint on communication condition are satisfied. This can be summarised as shown in Equation (1).

$$\text{Covert Channel Exists} \implies \text{Potential for Communication} \ \wedge \ \text{Constraint on Communication} \tag{1}$$

By taking the contrapositive of Equation (1), we obtain Equation (2).

$$\begin{aligned} &\neg(\text{Potential for Communication} \ \wedge \ \text{Constraint on Communication}) \implies \neg(\text{Covert Channel Exists}) \\ \iff \\ &\neg(\text{Potential for Communication}) \ \vee \ \neg(\text{Constraint on Communication}) \implies \neg(\text{Covert Channel Exists}) \end{aligned} \tag{2}$$

In general, Equation (2) illustrates how the necessary conditions for covert channel existence can be utilised for developing approaches for mitigating covert channels in systems of communicating agents. In particular, Equation (2) shows that if it can be shown that either of the necessary conditions for covert channel existence are not satisfied for a given system, then it is not possible for a covert channel to exist in that system. It is through Equation (2) that we form the basis of our proposed certification schema. Moreover, Equation (2) highlights two fronts from which the certification of covert channel freeness in cloud-based systems can be addressed. First, ways in which the potential for communication among system agents can be disrupted or eliminated by modifying and restricting agent behaviours in a given system can be explored. Second, a study of how to restrict the knowledge of the system agents on a potential communication path so that they are unable to know any fragments of confidential information that can be leaked via covert channels and then reconstituted by the receiver can be examined.

4.2. The Proposed Certification Schema

Certification refers to the ability to mathematical substantiate the non-existence of covert channels in the given system. In what follows, this comes in the form of a formal verification of the satisfiability of the necessary conditions for covert channel existence with respect to a given formal specification of a cloud-based system and a given security policy.

The proposed schema for certifying covert channel freeness in cloud-based systems is an application of the formal foundation laid out in our previous work [10,11,12,13]. Assume that we are given a cloud-based system formally specified using the mathematical framework of Communicating Concurrent Kleene Algebra [12] (C^2KA) which is an extension of Hoare et al.'s concurrent Kleene algebra [20] (CKA). C^2KA allows for the specification of the concurrent and communicating behaviour of agents in *open systems* with the notion of external stimuli coming from outside the boundaries of the system being considered. This capability is integral when considering the need to specify cloud-based systems, since the openness of the cloud is one of its central features. Cloud-based systems afford the ability for many agents to interact with one another without the existence of any clearly defined system boundaries. Furthermore, the potential for communication condition has been formulated [13] using C^2KA. Because of this, C^2KA provides the formal foundation upon which the proposed certification schema is built. The details of using C^2KA for specifying systems of communicating agents (e.g., cloud-based systems) can be found in Jaskolka et al. [11,12] and due to space limitations, they are not discussed any further in this paper. Further assume that we are given a security policy for the given specification which identifies the set of confidential information for each agent in the system. Then, the schema for certifying covert channel freeness in the given cloud-based system proceeds as follows.

Step 1: Formally Verify the Necessary Conditions for Covert Channel Existence. The first step is to formally verify the necessary conditions for covert channel existence with respect to the given security policy. The feasibility of verifying the necessary conditions for covert channel existence was outlined by Jaskolka et al. [10]. If it can be shown that either one of the necessary conditions for covert channel existence are not satisfied for the given system, then a certificate shall be issued indicating that the given system is free from covert channels. It is critical to note that only one of the necessary conditions for the existence of covert channels needs to be shown not to be satisfied in order to issue the certification. Conversely, if both of the necessary conditions for covert channel existence are satisfied, then a certificate shall not be issued. In this case, a report pointing to the behaviour or knowledge of the agent(s) which caused the certification to fail shall be provided. For example, such a report may include a list of all of the potential communication paths or "patterns of communication" that can exist between the system agents. The purpose of such a report is to point an analyst to ways in which the behaviour or knowledge of system agents can be amended, modified, or redesigned, in order to falsify the necessary conditions for covert channel existence. It should be noted that the details of generating such a report are not discussed any further in this paper.

Step 2: Amend, Modify, or Redesign the Behaviour or Knowledge of System Agents. The second step, which is necessary only if a certificate is not issued in Step 1, is to determine if and how the system may be amended, modified, or redesigned, in order to mitigate the potential for communication amongst system agents or to further restrict the knowledge of some system agents in an effort to work towards the development of a system that can be certified to be free of covert channels. After such amendments or modifications are made to the design of the system, the process can be repeated from Step 1 and the necessary conditions for covert channel existence can be verified again. More details regarding how an analyst may proceed with this step with respect to the falsification of the potential for communication condition are provided in Section 5.

5. Certification Through Falsification of the Potential for Communication Condition

As mentioned in Section 4.1, there are two fronts from which we can attack the problem of certifying covert channel freeness in cloud-based systems. Recall that if the certification of covert channel freeness for a given cloud-based systems fails, then it means that both of the necessary conditions for covert channel existence are satisfied. However, in order to issue the certification, only one of the necessary conditions for the existence of covert channels needs to be shown not to be satisfied. Because of this, throughout the remainder of this paper, we will focus only on the front established by the potential for communication condition. This is not to say that the proposed certification cannot be tackled from the front established by the constraint on communication condition; it is merely that it is often easier to think and reason about agent behaviour and the ways in which agents can potentially communicate with one another, rather than thinking and reasoning about agent knowledge and what agents can infer through their interactions. In this way, we simply reduce the problem of certifying covert channel freeness in cloud-based systems to eliminating the potential for communication among system agents.

According to Section 4.2, if a certificate of covert channel freeness is not issued for a given system, then a report indicating the communication paths or "patterns of communication" that have caused the certification to fail shall be provided. Given these communication paths that are possible in the given system, the analyst needs to identify ways in which the behaviour of system agents can be amended, modified, or redesigned in order to eliminate each potential communication path.

When examining how to amend or modify the behaviour of agents in a system in order to falsify the potential for communication condition, it is important to keep in mind the goal of disrupting or eliminating the potential for communication amongst system agents, while maintaining the normal operation of the system. It is obvious that the elimination of all possible forms of communication amongst agents in the system (i.e., achieving a completely isolated system) will indeed falsify the potential for communication condition and eliminate the possibility of covert channels. However, it is just as plain to see that the resulting system would be rendered useless, since a central feature of nearly all cloud-based systems is the communication and interaction of its agents. Instead, we aim to identify ways in which we can certify covert channel freeness in a system while still maintaining its overall behaviour. However, it is noted that this additional security may come at the cost of some other non-functional system requirements such as reliability or performance. This becomes a trade-off that must be reconciled by the system designers in order to achieve the desired system and its behaviour.

The problem of modifying the behaviour of agents in a given communication path in order to eliminate the potential for communication has been studied in previous work. Specifically, we showed[13] how the modification of agent behaviours in a communication path can preserve or disrupt the potential for communication in the given path. In this work, the potential for communication condition for covert channel existence is formulated using the mathematical framework of Communicating Concurrent Kleene Algebra[12] (C^2KA). This allows for the formulation of the potential for communication condition to consider communication via shared environments, as well as communication via external stimuli. In turn, this allows for the consideration of communication in open systems, which, as mentioned in Section 4.2, is an important part of analysing cloud-based systems for the existence of covert channels.

Intuitively, the results that we have previously presented[13] can guide an analyst in amending or modifying the behaviour of some system agents so that there is no longer a potential for communication between some agents in the system. As one example of modifying the system behaviour, consider a cloud-based system for which agents issue transaction requests to the cloud and where acknowledgements are directly sent to other system agents after a transaction has been completed. Furthermore, suppose that it is possible for agents to control the timing of the acknowledgements that are issued to other system agents, thereby affording the possibility to establish a timing-based covert channel. In an attempt to eliminate the potential for communication amongst the agents in this system, while still preserving its overall behaviour, it is possible to inject a filtering agent that all of the communication between agents must pass through, for example. The purpose of such an agent is to de-couple any direct potential for communication between an agent knowing some confidential information and an agent that is not permitted to know that information. In this way, the filtering agent can be used to issue acknowledgements immediately after receiving a transaction request so that the system agents no longer have any control over the timing of the acknowledgements. Such a filtering agent needs to be carefully designed so as not to introduce new covert channels. However, as mentioned earlier, this solution can run into some practical problems. Since the proposed solution finds the filtering agent

issuing acknowledgements immediately after it receives a transaction request from an agent, the system agent cannot confirm that the requested transaction was in fact completed. Instead, they must simply trust that the cloud services are functioning properly and completing the requested transactions. This highlights the point that in order to attain higher levels of security, there are potential tradeoffs with regard to the reliability, and possibly other non-functional requirements of the system[21]. Therefore, while some solutions for mitigating the existence of covert channels in cloud-based systems can protect the system's confidential information and maintain its overall behaviour, they often come at a cost of reduced system reliability and performance.

In some cases it may not be possible to eliminate the communication between some system agents while still achieving some other high priority non-functional requirements such as performance or reliability. In these cases, assuming that it is also not possible to restrict the knowledge of the systems agents in such a way to falsify the constraint on communication condition, it is clear that a certification of covert channel freeness cannot be issued. However, it may be possible to use the proposed schema to at least guide an analyst in redesigning the system in such a way that the communication amongst system agents cannot proceed in an unexpected way which would thereby allow for the establishment of a covert channel. As mentioned earlier, it is through these unexpected uses of system resources and functionalities that covert channels are possible. For instance, an analyst may design the system such that agents may only communicate via external stimuli in a form of message-passing communication. In this way, the analyst can ensure (via formal verification of the potential for communication[13]) that there is no means to communicate via a shared environment. Therefore, while the potential for communication condition is still satisfied, it then becomes possible to observe the communication amongst these system agents to ensure that the security policy is being respected. For example, in order to detect confidential information leakage, monitors can be installed and configured to identify "patterns of communication" on the communication channels available to the agents in a potential communication path using techniques similar to those presented by Jaskolka et al.[22,23]. Similarly, mechanisms can be used to de-couple or deteriorate any sort of timing information associated with the communication channels available to the agents in the potential communication path by injecting random delays similar to the approach taken by the NRL Pump[24].

6. Concluding Remarks

In this paper, without discussing all of the details of the formal specification of cloud-based systems and the formal verification of the necessary conditions for covert channel existence due to space limitations, we outlined a schema for certifying covert channel freeness in cloud-based systems. The proposed schema provides an application of the formal foundation laid out in our previous work[10,11,12,13]. It is based on a strategy derived from the necessity and formal verification of the conditions for covert channel existence in cloud-based systems specified using the mathematical framework of Communicating Concurrent Kleene Algebra (C^2KA). We also discussed how the problem of certifying covert channel freeness in cloud-based systems can be tackled by looking only to the falsification of the potential for communication condition. In this discussion, we pointed to existing work which can be used as part of the proposed certification strategy for identifying ways in which an analyst may amend, modify, or redesign a system in order to make it more resilient to covert channels, and to potentially certify it to be free from covert channels on the basis of the non-existence of the potential for communication amongst its agents.

The proposed schema for the certification of covert channel freeness in cloud-based systems is a step towards the mitigation of confidentiality concerns surrounding cloud computing. It provides a means for assuring covert channel freeness at early stages in the development of the system, namely at the system specification level. However, it is uncertain how the proposed certification schema, in its current form, will scale to handle large cloud-based systems with numerous interacting agents, each with a significant amount of information contained in their respective data stores, and being exchanged amongst them. In this paper, we looked particularly at a schema for formally certifying covert channel freeness in cloud-based systems through an examination of the front established by the potential for communication condition. However, it is possible to also consider the problem from the front established by the constraint on communication condition. This would involve a formulation of the constraint on communication condition, the formal specification of agent knowledge, and the ability to reason about what an agent knows, or can come to know, through its interaction with other agents in the system. This can be done using a formalism such as description logic[25].

In our current and future work, we aim to develop tool support that can aid in the automation of the proposed certification schema. This involves the automation of the verification of the necessary conditions for covert channel

existence, as well as the issuance of certificates. Additionally, as mentioned in Section 4.2, in the case when a certificate is not issued, we look to automate the generation of a report indicating the reasons for failing the certification. For example, such a report can include an automatically generated list of each of the possible communication paths between agents in a given system.

With the increasing popularity of cloud-based systems and the growing concerns surrounding security and privacy in today's society, the need for mechanisms for mitigating the threat of confidential information leakage and subsiding the surrounding concerns is more important than ever. The schema for certifying covert channel freeness in cloud-based systems proposed in this paper is merely one step towards this goal.

Acknowledgements

This research is supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) through the grant RGPIN 2014-06115.

References

1. Zissis, D., Lekkas, D.. Addressing cloud computing security issues. *Future Generation Computer Systems* 2012;**28**(3):583–592.
2. Buyya, R., Broberg, J., Goscinski, A.. *Cloud Computing: Principles and Paradigms*; vol. 81 of *Wiley Series on Parallel and Distributed Computing*. John Wiley & Sons; 2011.
3. Milner, R.. *Communication and Concurrency*. Prentice-Hall International Series in Computer Science. Prentice Hall; 1989.
4. Krutz, R., Vines, R.. *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. John Wiley & Sons; 2010.
5. Wu, Z., Z. Xu, Z., Wang, H.. Whispers in the hyper-space: High-bandwidth and reliable covert channel attacks inside the cloud. *IEEE/ACM Transactions on Networking* 2014;**PP**(99):1–1.
6. U.S.A. Department of Defense, . *Trusted Computer System Evaluation Criteria (TCSEC)*. No. DoD 5200.28-STD in Defense Department Rainbow Series (Orange Book). Fort George G. Meade, MD, U.S.A.: Department of Defense/National Computer Security Center; 1985.
7. Simmons, G.. The subliminal channel and digital signatures. In: Beth, T., Cot, N., Ingemarsson, I., editors. *Advances in Cryptology*; vol. 209 of *Lecture Notes in Computer Science*. Springer Berlin/Heidelberg; 1985, p. 364–378.
8. Murdoch, S.. Covert channel vulnerabilities in anonymity systems. Tech. Rep. UCAM-CL-TR-706; University of Cambridge; Cambridge, UK; 2007.
9. Jaskolka, J., Khedri, R.. Exploring covert channels. In: *Proceedings of the 44th Hawaii International Conference on System Sciences*; HICSS-44. Koloa, Kauai, HI, U.S.A.; 2011, p. 1–10.
10. Jaskolka, J., Khedri, R., Zhang, Q.. On the necessary conditions for covert channel existence: A state-of-the-art survey. *Procedia Computer Science* 2012;**10**:458–465. Proceedings of the 3rd International Conference on Ambient Systems, Networks and Technologies, ANT 2012.
11. Jaskolka, J., Khedri, R., Zhang, Q.. Foundations of communicating concurrent Kleene algebra. Tech. Rep. CAS-13-07-RK; McMaster University; Hamilton, ON, Canada; 2013. Available: `http://www.cas.mcmaster.ca/cas/0template1.php?601`.
12. Jaskolka, J., Khedri, R., Zhang, Q.. Endowing concurrent Kleene algebra with communication actions. In: Höfner, P., Jipsen, P., Kahl, W., Müller, M., editors. *Proceedings of the 14th International Conference on Relational and Algebraic Methods in Computer Science*; vol. 8428 of *Lecture Notes in Computer Science*. Springer International Publishing Switzerland; 2014, p. 19–36.
13. Jaskolka, J., Khedri, R.. A formulation of the potential for communication condition using C^2KA. In: Peron, A., Piazza, C., editors. *Proceedings of the 5th International Symposium on Games, Automata, Logics and Formal Verification*; vol. 161 of *Electronic Proceedings in Theoretical Computer Science*. Verona, Italy: Open Publishing Association; 2014, p. 161–174.
14. Ristenpart, T., Tromer, E., Shacham, H., Savage, S.. Hey, you, get off of my cloud! Exploring information leakage in third-party compute clouds. In: Jha, S., Keromytis, A., editors. *Proceedings of the 16th ACM Conference on Computer and Communications Security*; CCS 2009. ACM Press; 2009, p. 199–212.
15. Salaün, M.. Practical overview of a Xen covert channel. *Journal in Computer Virology* 2009;**6**(4):317–328.
16. Cabuk, S., Brodley, C., Shields, C.. IP covert channel detection. *ACM Transactions on Information and Systems Security* 2009;**12**(4).
17. Mehmood, A., Song, H., Lloret, J.. Multi-agent based framework for secure and reliable communication among open clouds. *Network Protocols and Algorithms* 2014;**6**(4):60–76.
18. Smeets, M., Koot, M.. Research report: Covert channels. Tech. Rep.; University of Amsterdam; Amsterdam, Netherlands; 2006.
19. Bidou, R., Raynal, F.. Covert channels. 2005. URL: `http://www.iv2-technologies.com/~rbidou/CovertChannels.pdf`.
20. Hoare, C., Möller, B., Struth, G., Wehrman, I.. Concurrent Kleene algebra and its foundations. *Journal of Logic and Algebraic Programming* 2011;**80**(6):266–296.
21. Moskowitz, I., Kang, M.. Covert channels — here to stay? In: *Computer Assurance*; COMPASS '94 Safety, Reliability, Fault Tolerance, Concurrency and Real Time, Security. Gaithersburg, MD , U.S.A.: IEEE Computer Society; 1994, p. 235–243.
22. Jaskolka, J., Khedri, R., Sabri, K.. A formal test for detecting information leakage via covert channels. In: *Proceedings of the 7th Annual Cyber Security and Information Intelligence Research Workshop*; CSIIRW7. Oak Ridge, TN, U.S.A.; 2011, p. 1–4.
23. Jaskolka, J., Khedri, R., Sabri, K.. Investigative support for information confidentiality part I: Detecting confidential information leakage via protocol-based covert channels. In: *Proceedings of the 9th International Conference on Future Networks and Communications*; vol. 34 of *Procedia Computer Science, FNC 2014 and MobiSPC 2014*. Niagara Falls, ON, Canada; 2014, p. 276–285.
24. Kang, M., Moskowitz, I.. A pump for rapid, reliable, secure communication. In: *Proceedings of the 1st ACM Conference on Computer and Communications Security*. Fairfax, VA, U.S.A.; 1993, p. 119–129.
25. Baader, F., McGuinness, D., Nardi, D., Patel-Schneider, P., editors. *The Description Logic Handbook: Theory, Implementation, and Applications*. Cambridge University Press; 2003.