Petri net modeling of encrypted information flow in federated cloud

Abdul Rauf Khushk¹ and Xiaozhong Li²,∗
¹College of Economics and Management, Tianjin University of Science and Technology, Tianjin 300222, China
²College of Computer Science and Information Engineering, Tianjin University of Science and Technology, Tianjin 300222, China, E-mail: lixz@tust.edu.cn
*Corresponding author

Abstract. Solutions proposed and developed for the cost-effective cloud systems suffer from a combination of secure private clouds and less secure public clouds. Need to locate applications within different clouds poses a security risk to the information flow of the entire system. This study addresses this by assigning security levels of a given lattice to the entities of a federated cloud system. A dynamic flow sensitive security model featuring Bell-LaPadula procedures is explored that tracks and authenticates the secure information flow in federated clouds. Additionally, a Petri net model is considered as a case study to represent the proposed system and further validate the performance of the said system.

1. Introduction
Recently, lots of combined systems are being introduced, proposed and developed to overcome the security issues of different organizations. For large organizations, data and information are very important to be protected so federated cloud system with combined Petri nets and other system integrated into it made a promising security system to protect data and information [1, 5]. Moreover, large organizations demands of keeping sensitive information on their more limited servers rather than in the public cloud which outlined the Federated Cloud Computing (FCC) in which both public and private cloud computing properties are used [2]. Likewise, the development of federated cloud system (FCS) with a different model of Petri nets modeling according to the needs of industries and several organizations for accessing the data and information and several applications are still being developed concerning the security policies. FCS has been more reliable as well as cost effective but the security risks of protecting data and information are still a big problem. Hence, minimizing and to overcome these security risk problems tracking and controlling of data and information flow in the system is essential [3]. So, a novel model system must be developed describing the information and tracking the flow of data and information [5].

Following the federated cloud systems, many models have been emerged with different methods of workflow security such as Petri nets especially to model the workflow integrating Bell-LaPadula model to workflow security which can be also called as the flow-sensitive analysis of programs[4]. But these kinds of models can only read and write policies having several drawbacks. Moreover, some of the Bell-LaPadula integrated models failed to get clearance for location level. Thus, realizing these several drawbacks and problems that occurred in different previous models developed which still lack protecting the securities policies. So, our research and dedication for developing a new combined model of federated intensively affect the information flow security of the entire system. In this paper, we present the user security levels for a distributive dynamic flow sensitive security model applying read with
decryption and write with encryption in cloud system can be very promising and much more advantageous for overcoming the security risks.

Like industry standards such as UML activity diagrams, Business Process Model and Notation and EPCs, Petri nets offer a graphical notation for stepwise processes that include choice, iteration, and concurrent execution. Unlike these standards, Petri nets have an exact mathematical definition of their execution semantics, with a well-developed mathematical theory for process analysis [Carl Adam Petri].

In this study, we proposed a formal model of colored Petri Nets in which partition of workflows over a set of accessible clouds to meet maximum security requirements which are significantly based on a multi-level security model that extends Bell-LaPadula to encompass cloud computing [6]. We have used Colored Petri Nets (CPNs) to capture the flow of information flow in federated cloud computing systems, as well as the clouds and services, are fixed by applying decryption method in read and encryption method in write. Moreover, we focused on locating various kinds of data resources and users inside the formal model system. Several modifications and movements are not considered such as server-side components and dynamic movements, the execution of tasks in the system [7] etc. This formal model especially designed to capture the distributive dynamic information flow-sensitive security, where subjects (services) and objects (data) can migrate and change their security status dynamically.

2. Formal Model of Petri Nets Representing Distributive Dynamic Flow –Sensitive Security

Usually, a basic Petri Net (N) consists of two types of nodes, Pl and Tr, respectively called places and transitions, a set F ∈ (Pl×Tr) ∪ (Tr×Pl) of arcs that connect the nodes, and the initial marking M0 : Pl → N which is a mapping from the set of places to the set N of all non-negative integers [11].

As per the information lattice for security concerns, Lsec = (Lsec, ≤sec) consists of a set Lsec and a partial order relation≤sec such that, for all Ɩ, Ɩʹ ∈ Lsec, there exists a least upper bound l∪lʹ ∈ Lsec, and a greatest lower bound l∩lʹ ∈ Lsec [8,10].

Bell-LaPadula (1973) discovered a multi-level control security model which consist of five components such as (i) a set of possible access rights R, (ii) a complete lattice for security concern Lsec = (Lsec, ≤ sec), (iii) an access control matrix: B: S×O → 2R, (iv) a security level map: l: E → Lsec and (v) an ordered set over the set of tuples M.

For an effective and efficient Petri net formal model, we have integrated all the basic requirements of components such as information lattices, Bell-LaPadula and cloud security described as below;

Definition (DDFSSM): A Distributive dynamic flow-sensitive security model for federated clouds is a tuple:

\[ \text{DDFSSM} = (S_{\text{ency}}, O_{\text{decr}}, L_{\text{sec}}, A, \text{st}_{\text{init}}) \]

S is a finite non-empty set of encryption subjects/encryption services, O is a finite non-empty set of decryption objects/decryption data, Lsec is a complete security lattice, A is a finite set of actions partitioned into three sets, each action being a pair (φ^out_{\text{ency}} φ^out_{\text{decr}}) Consisting of two finite multi- sets over the set of tuples M = S_{\text{ency}} × L_{\text{sec}} × L_{\text{sec}} × X ⊆ O_{\text{decr}} × L_{\text{sec}} × X, where st_{init} is an initial state defined as a finite multi-set over the set of tuples M.

In general, a state of DDFSSM is a finite multi-set over the set of tuples M.

Considering the above concept we have proposed a formal Petri nets model as in figure (1). A tuple (s, l, c, x) ∈ S_{\text{ency}} × L_{\text{sec}} × L_{\text{sec}} × X, later signified by (s, l, c) @ x, represents an encryption service (s) with the security level (l) and the clearance level (c) (c ≥ sec l) residing on cloud p. Similarly, a tuple (o, l, p) ∈ O_{\text{decr}} × L_{\text{sec}} × X, later signified by (o, l)@x, represents a decryption data item (o) with the security level l residing on cloud x. a set place followed by a set of transition such as places (P):(P1.P2.P3, P4,
P5) and transitions(T): (T1, T2,,T11). Moreover, the initial marking as $M_0(0,1,0,0,0)$. The set of input and output in the system is done by the matrix for as in table (1). Set of Initial $M_0$ {P1=0,P2=1,P3=0,P4=0,P5=0} and the result is $M_0(01000)$.

**Table 1.**  Representation of a set of input and output in matrix order.  

|       | T1 | T2 | T3 | T4 | T5 | T6 | T7 | T8 | T9 | T10 | T11 |
|-------|----|----|----|----|----|----|----|----|----|-----|-----|
| P1    | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0   | 0   |
| P2    | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 1  | 0   | 0   |
| P3    | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0   | 0   |
| P4    | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 1   | 1   |
| P5    | 0  | 1  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0   | 0   |

|       | T1 | T2 | T3 | T4 | T5 | T6 | T7 | T8 | T9 | T10 | T11 |
|-------|----|----|----|----|----|----|----|----|----|-----|-----|
| P1    | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0   | 0   |
| P2    | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 1   | 1   |
| P3    | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0   | 0   |
| P4    | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 0  | 0   | 1   |
| P5    | 1  | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 0   | 1   |

**Figure 1.** Shows the structure of the access control subnet (a central component of the Petri net model), representing the behavior of the subjects and objects residing on the same cloud (for simplicity, transitions relating to data destruction and creation have been omitted). circle denotes place from where token is fired and square box represents transition of fired token.
We take a persistent storage system with CRUD (create, retrieve, update, and delete) interface as an example, shown in figure 1, that highlights the importance of incorporating security infrastructure in clouds. We consider two public clouds, X0 and X1, and one private cloud, X2. Services and data can be deployed on different clouds, both services s0 and s1 can be deployed on X0, X1 and X2. However, the data item X0 can only be deployed on cloud X2. The left most sub-net (control flow subnet) shows how the services can migrate between different clouds under the security policy represented by the guards of the form $l \leq \sec c \leq \sec l X1$ associated with the transitions. The data resources are represented by a single token, $(d0, 1)@X2$, inside another place labeled X2 (belonging to the data flow sub-net). It follows from the security levels of the data resources and clouds that such a resource can never enter X0 or X1. Note also that the security policy for data migration is represented by the guards of the form $l \leq \sec l(X0)$ associated with the transitions in the data flow sub-net.

3. Conclusions
In conclusion, we presented a Petri net distributive dynamic flow-sensitive security model which can be used to analyze the information flow in federated clouds with encryption and decryption method. The entities present in the cloud system can be assigned different security levels belonging to a given security lattice. Furthermore, each cloud is assigned a security level which captures the confidentiality level of the cloud. It is also potential to specify in a formal way different security strategies for the movement of entities between different clouds. The resulting formal model can then be represented by a suitable colored Petri net, and its dynamic properties analyzed using the existing verification methods and tools developed for Petri nets.

4. Acknowledgement
This work was supported by National Natural Science Foundation of China Grant Nos. 11301382 and 61603273, by Tianjin Application Foundation and Advanced Technology Research Project under Grant No. 14JCQNJC00300, and by Natural Science Foundation of Tianjin under Grant No. 16JCYBJC18500.

5. References
[1] W. Zeng, C. Mu, M. Koutny, and P. Watson, “Formal verification of secure information flow in cloud computing Workshop on information security applications, 2016: 103-116.
[2] P. Watson, “A multi-level security model for partitioning workflows over federated clouds,” Journal of Cloud Computing, vol. 1, no. 1, pp.1–15, 2012.
[3] W. Zeng, C. Mu, M. Koutny, and P. Watson, “verifying secure information in federated Clouds 2014 IEEE 6th International Conference on Cloud Computing Technology and Science
[4] G. Smith, “A new type system for secure information flow,” in In CSFW14. IEEE Computer Society Press, 2001, pp. 115–125.
[5] W. Zeng, C. Mu, M. Koutny, and P. Watson, “A flow-sensitive security model for cloud Computing systems,” CoRR, vol. abs/1404.7760, 2014.
[6] K. Knorr, “Dynamic access control through Petri net workflows,” in Proceedings of the 16th Annual Computer Security Applications Conference, ser. ACSAC ’00, 2000, pp. 159–167.
[7] W. Zeng and M. Koutny, “Data resources in dynamic environments,” in IEEE 8th International Symposium on Theoretical Aspects of Software Engineering (TASE), 2014.
[8] D. E. Denning, “A lattice model of secure information flow,” Commun.ACM, vol. 19, pp. 236–243, May 1976.
[9] J. Landauer and T. Redmond, “A lattice of information,” in Computer Security Foundations Workshop VI, 1993. Proceedings, Jun 1993, pp.65–70.
[10] N. A. Electronic, L. Lapadula, T. Original, D. E. Bell, and L. J. Lapadula, “Secure Computer Systems: Mathematical Foundations,” 1973.
[11] W. M. P. V. der Aalst, “Petri-net-based workflow management software,” in Proceedings of The NFS Workshop on Workflow and Process Automation in Information Systems, 1996, pp. 114–118.