A Knowledgebase Insider Threat Prevention Model in a Cloud Data Center

Rami Mohawesh
Qutaibah Althebyan
Qussai Yaseen
Yaser Jararweh
Jordan University of Science and Technology

Outline

- Introduction
- Insider Threat in the Cloud
- Fat Tree Cloud Architecture
- Insider Threat Knowledgebase
- Knowledge Graph
- Insider Threat Risk
- Insider Threat Example
- Insider Threat Proposed Model
- Model Overall Picture
- Experimental Results
- Conclusions and Future Work

Introduction

- Most security related research of cloud computing focuses on attacks generated outside the cloud system
  - Mainly tackles attacks trying to gain unauthorized access to the cloud resources and data
- Although such kind of attacks are important, however;
  - Little research focuses on a more sever kind of attacks of the cloud
    - The Insider Attacks

Introduction

- Security issues of insiders within the cloud have different angles:
  - Insiders are personnel who have authorized access privileges of cloud resources
  - Insiders have exact knowledge of all cloud resources; including but not limited to
    - Values and/or content
    - Location
    - Dependency
    - To whom it belongs to
    - Etc.
  - Insiders constitute huge number of privileged individuals
  - Different cloud insiders (if collaborating) might have access to cloud data of organizations who have conflict of interests (COI)

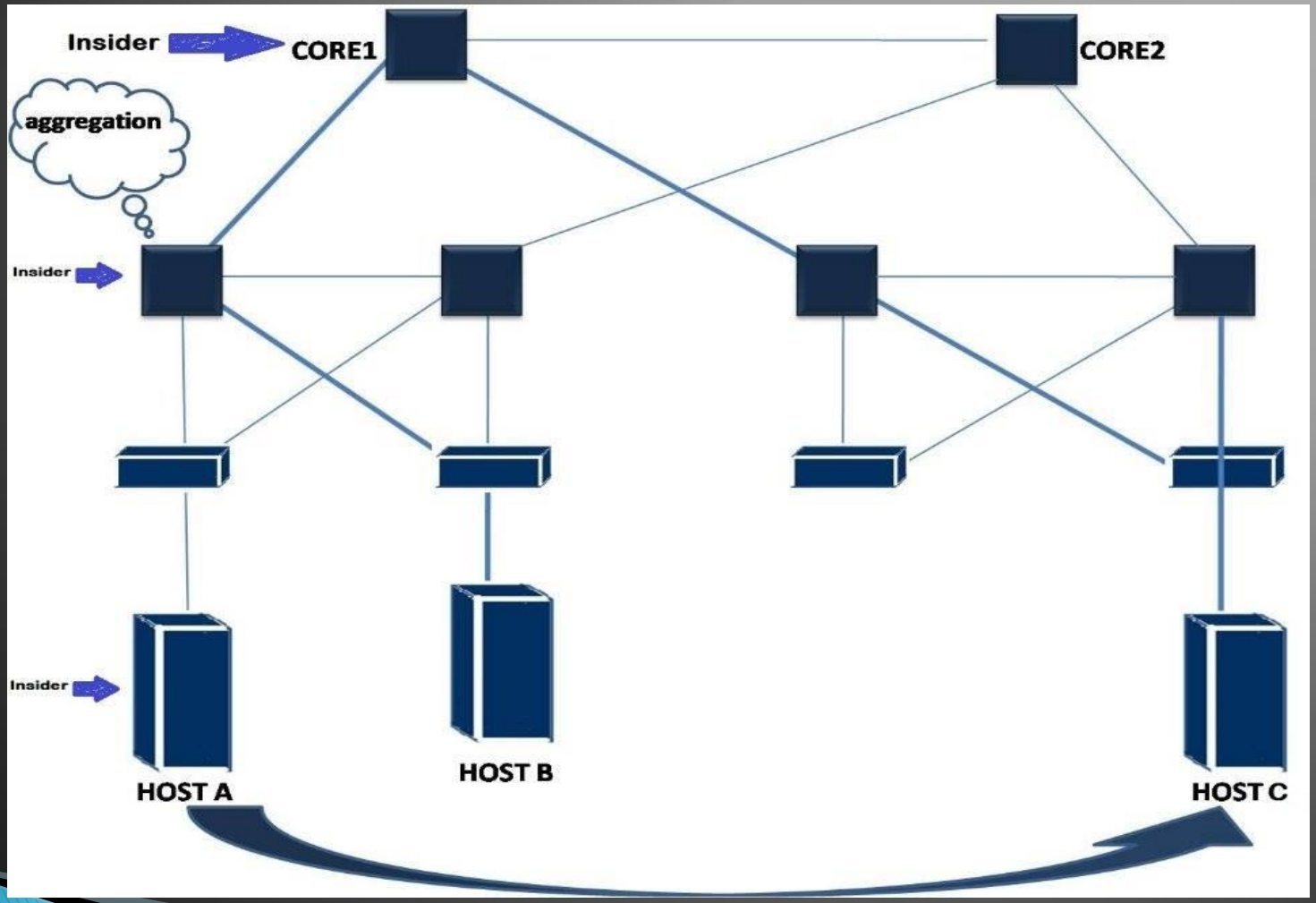
Introduction

- Proposed a novel insider threat detection and prevention model using knowledgebase prevention approaches.
  - Used our experience in knowledge base of insider threats mitigation at both the system and DB levels and extended this work to critical cloud computing system
  - The proposed model will insure an early detection and prevention of possible insiders' breaches

Insider Threat in the Cloud

- Follow the fat tree network architecture of the cloud
  - A very common architecture
- Distinguish three different kinds of insiders
  - Host Insiders: DB access privileges
  - Aggregated Insiders: DB access and network traffic privileges
  - Core Insiders: DB access and network traffic privileges

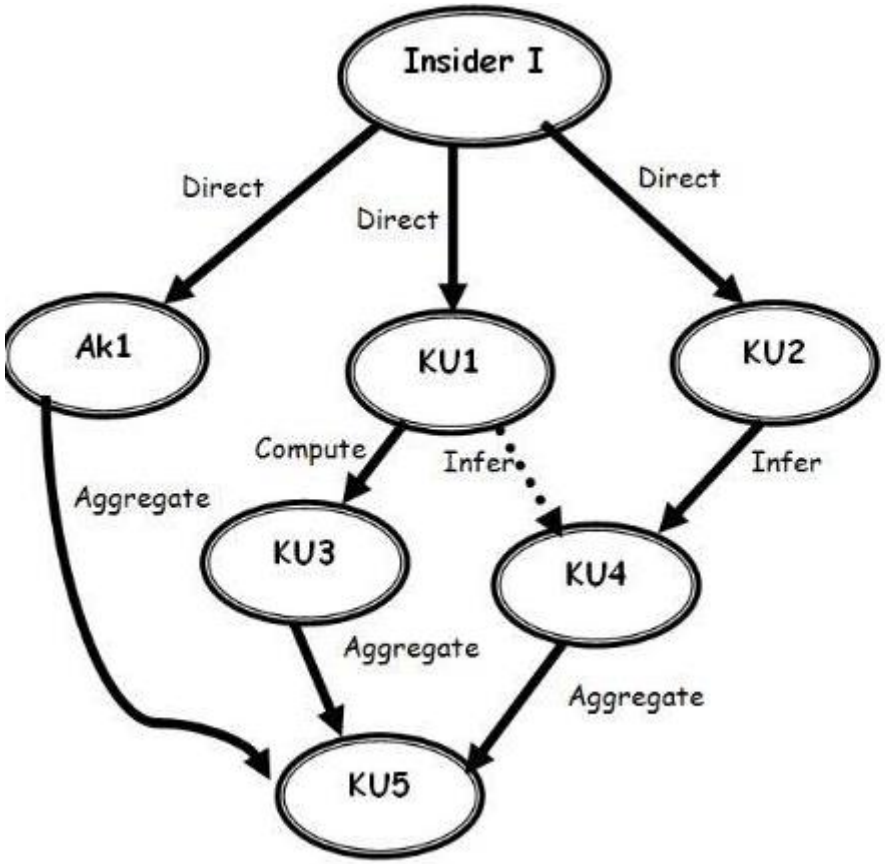
Fat Tree Cloud Architecture



Insider Threats Knowledgebase

- Insiders accumulate knowledge
  - Through their valid and authorized accesses
- This accumulated knowledge will be stored in a knowledgebase which represents:
  - Access history of insiders to data items as well as the values they read.
  - The knowledge the insider gains about the network traffic that he/she is eligible to watch.
    - Depending on his level and privileges

Knowledge Graph



Insider Threat Risk

- Risk comes from the fact that an insider may combine the value of a data item he/she has newly requested with the value of a data item that he/she had accessed before (which exists in his/her knowledgebase) to deduce values of other data items, which the user is not authorized to.
  - This is achievable using dependencies that exist among data items (in the form of databases) that exist in different levels especially in the host nodes.

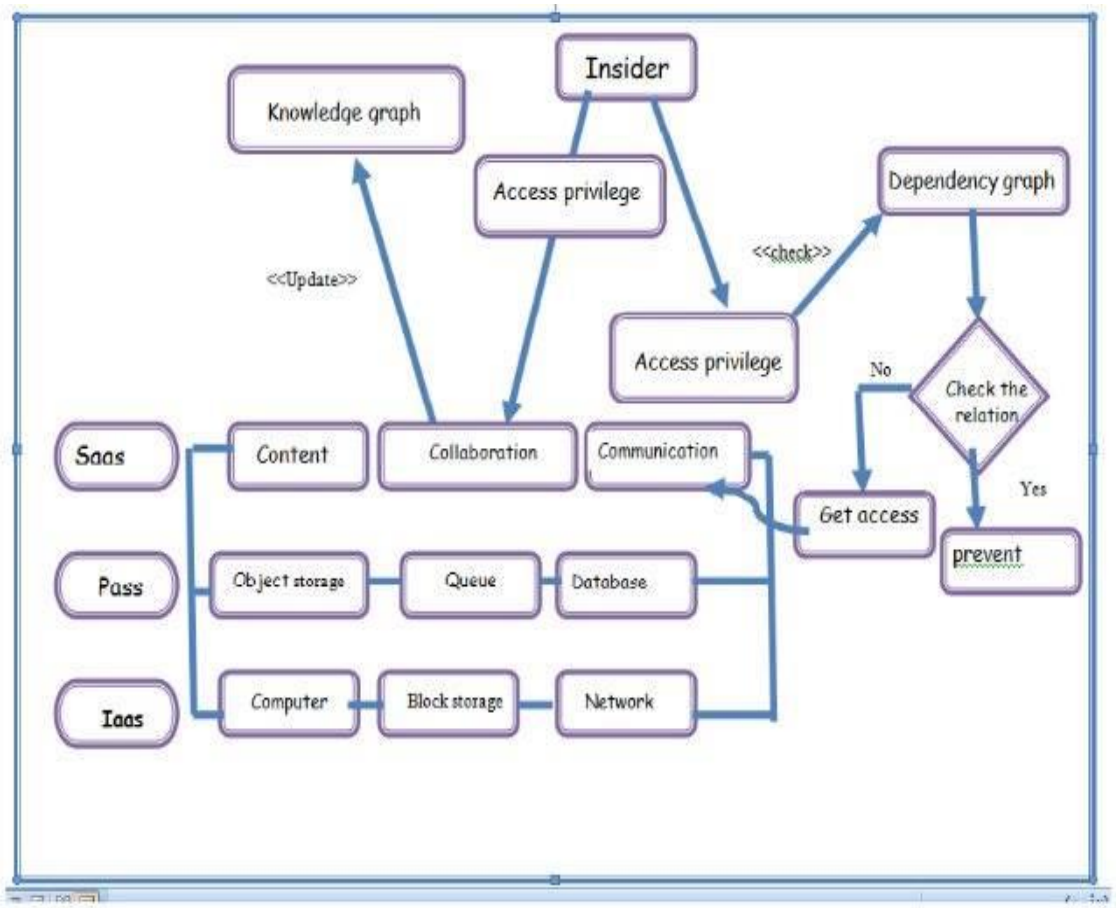
Insider Threat Example

- An aggregated insider has privileges in two hosts: Host A and Host B.
- This insider can use his privileges to accumulate knowledge about the databases in both hosts to infer some knowledge about some data items that exist in another host, say Host C, which he does not have access to.
- This is achievable
  - Dependencies among objects in Host A and Host B and the insider through his/her role can easily achieve this dependency knowledge.

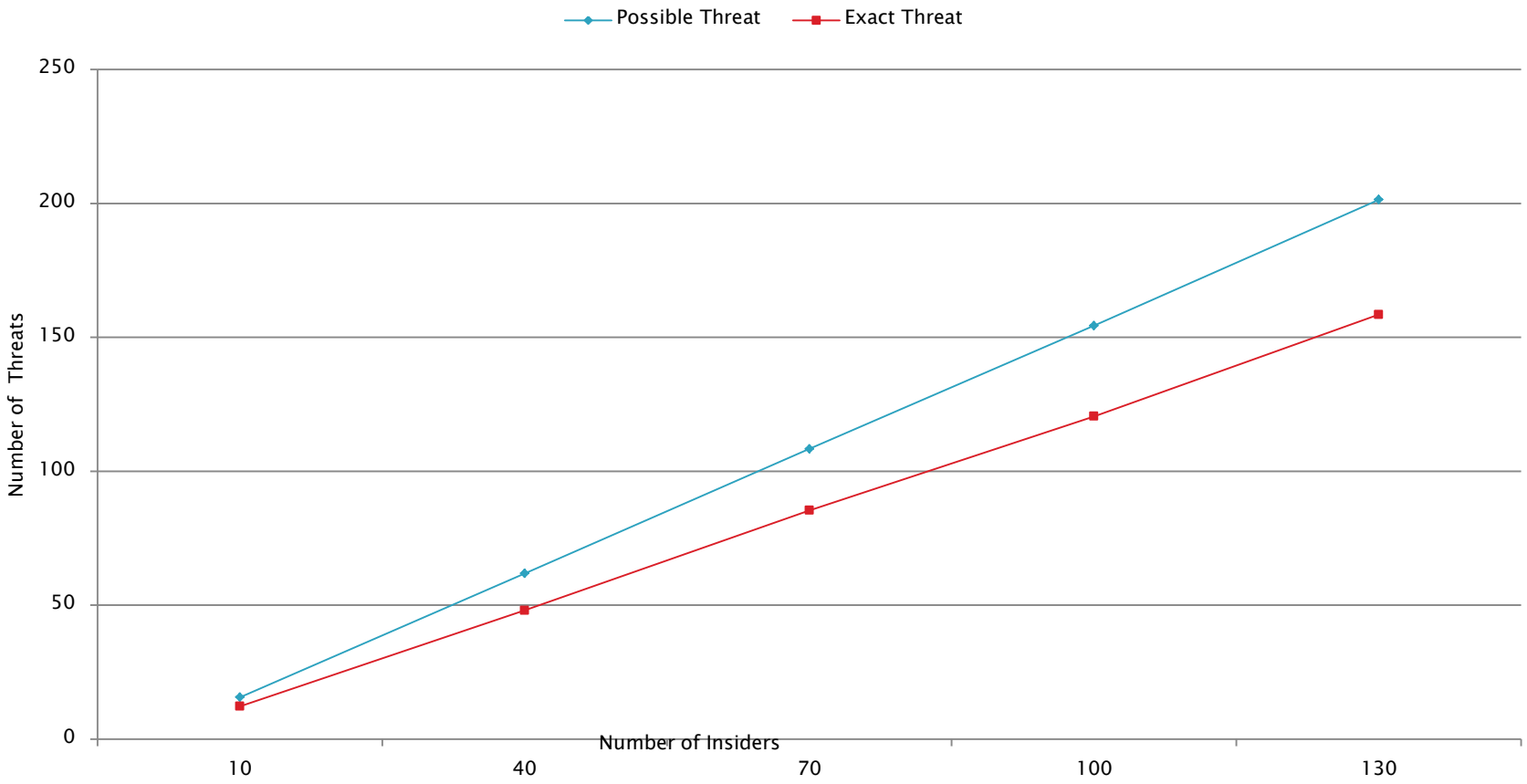
Insider Threat Proposed Model

- Built an Insider Threat Prevention model with:
  - Knowledge graph component: Tracks Insiders' accumulated knowledge
  - Dependency graph component: gives an overall image of different dependencies that exist among different objects
  - Detection/Prevention component: tracks insiders' activities
    - Raises an alarm if the knowledge of an insider will be increased (by valid accesses) to a point that might pose a threat to other comonent(s) that he is not authorized to

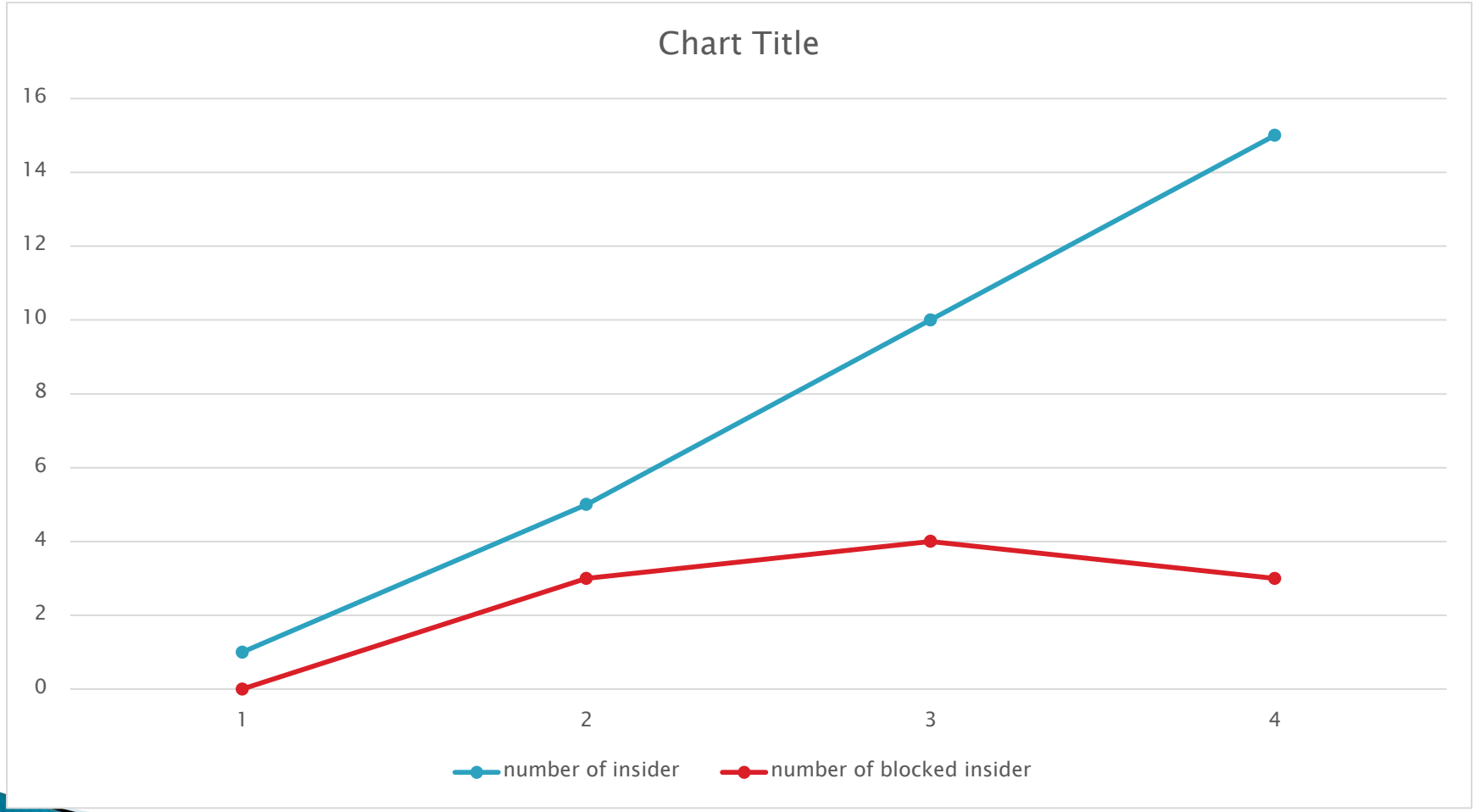
Model Overall Picture



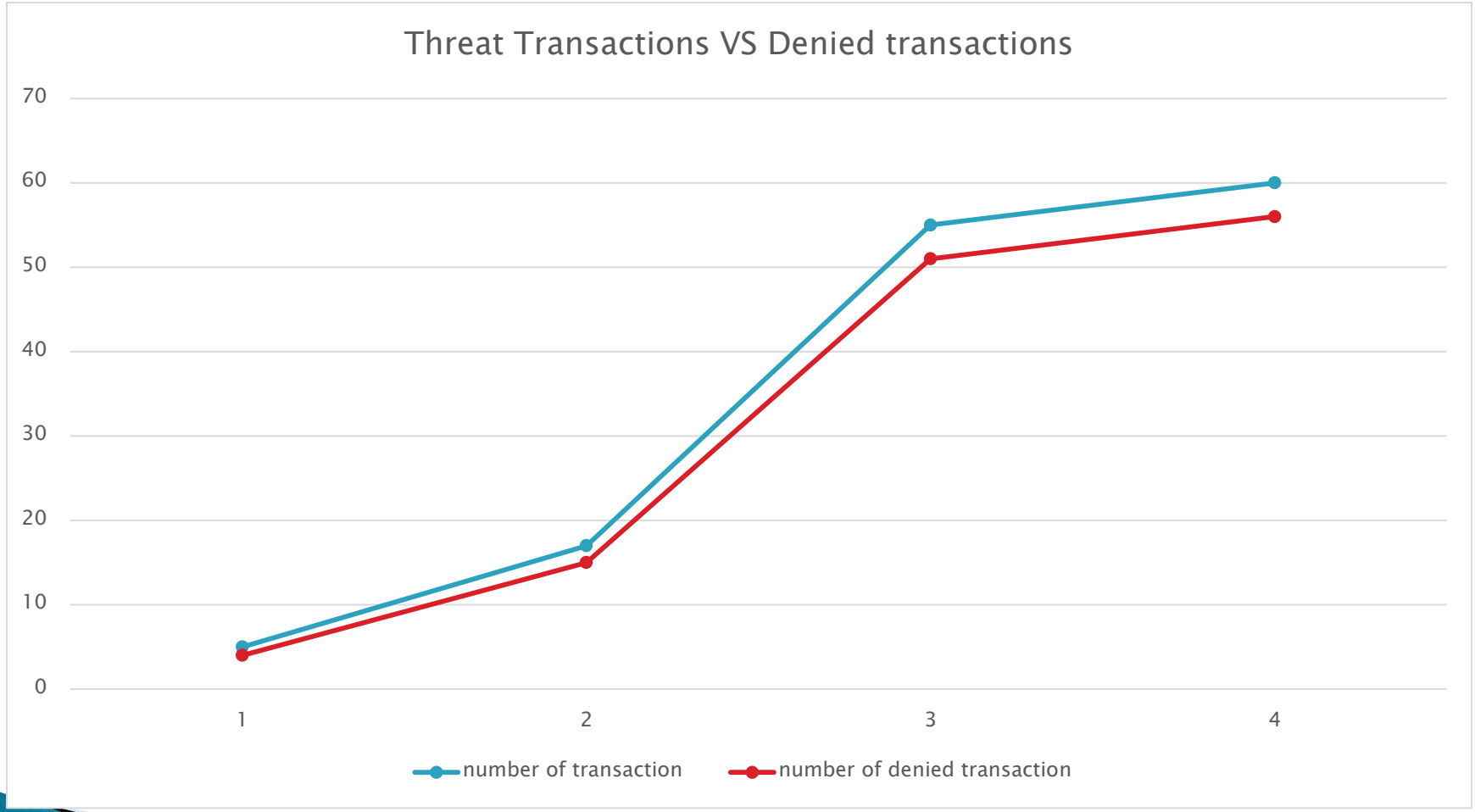
Experimental Results



Experimental Results



Experimental Results



Conclusions and Future Work

- Proposed a new insider threat detection and prevention model for the cloud datacenter
- Measured the effectiveness of the proposed model considering different scenarios
- Extend the presented model to consider the network traffic knowledge that both the aggregated and core insiders can gain

Questions