Cloud Technologies: Connected and Unconnected, yet Processing

CHAIR
Aspen Olmsted
Panel

Chair
• Aspen Olmsted, New York University, USA

Panelists
• Jiye Yu, Hitachi, Ltd., Japan
• Sebastian Fischer, Fraunhofer AISEC, Germany
• Bob Duncan, University of Aberdeen, United Kingdom
• Magnus Westerlund, Arcada University of Applied Sciences, Finland
Panel Chair

- 25 years in Industry Developing N-Tier Business Solutions
- Program Director and Professor at Fisher College in Boston
- Acting Program Director for New York University Cyber Fellows Program
- Research is in N-Tier and Cloud Application Correctness
Issues

• Synchronization of data and configuration between
  • Cloud and clients
  • Cloud VMs
• Stability of Connections
  • Latency
  • Reliability
• Privacy of Data over Connections
More Issues

• Processing
  • In Cloud
  • At Client

• Integrity when Systems are reconnected
  • Which version wins
  • Versioning levels
Cloud Improves Availability but does it also allow us to improve Integrity and Confidentiality

Aspen Olmsted, Fisher College & New York University, USA aolmsted@fisher.edu

- During COVID, K-12 and Higher Education Moved to Cloud and Remote
- News Media Focuses on challenges and Failures
- NYU has created an Online Cybersecurity MS degree with connections that cannot be offered in brick and mortar
- edX MicroBachelors offers undergraduate credits for high-quality low-cost education in the cloud
- This is a model for how many businesses can improve the integrity and confidentiality in other domains

→ COVID and Cloud will change how we do business
→ Integrity and confidentiality will be higher utilizing cloud and remote
→ Old models were inefficient
System Operator: Managing Kubernetes Operators for Your System

Jiye Yu, Hitachi, Ltd., Japan, jiye.yu.kb@hitachi.com

- Kubernetes and Operator
- System Operator to manage the whole Kubernetes system
- Deployment, upgrade, monitoring and backup
- Make policy on system level by monitoring data

→ Extend the ability of Kubernetes Operators
→ System Operator for Kubernetes
Cloud Technologies provide a huge diversity of services, but they lack IT-Security. Especially, with the growing amount of IoT devices, the security (and privacy) challenges are getting more and more...

Sebastian Fischer, Fraunhofer AISEC, Germany, sebastian.fischer@aisec.fraunhofer.de

- Baseline IT-Security
- Internet of Things (IoT) Security
- IoT Services
Panellist Position

The Complexities of Modern Cloud and the Impact on Compliance

Bob Duncan, University of Aberdeen, bobduncan@abdn.ac.uk

• Cloud security
• Corporate compliance
• Blockchain and the forensic trail
• Accountability

→ IoT security is hard to balance due to complexity and untrained users
→ Removing a need for centralized control of security is an opportunity for distributed systems
→ Autonomous Systems require Autonomous Security
Distributed security for distributed architectures

Magnus Westerlund, Arcada University of Applied Sciences, Helsinki, Finland

- Blockchain enforced security model
- Autonomous IoT devices
- Fleet monitoring
- Towards distributed security

→ IoT security is hard to balance btw complexity and untrained users
→ Removing a need for centralized control of security is an opportunity for distributed systems
  → Autonomous Systems require Autonomous Security
Cloud Computing 2020

Cloud Technologies: Connected and Unconnected, yet Processing
(cloud technological impact, service reliability, challenges for data and processes, trusted and secured environments, etc.)

Aspen Olmsted, Ph.D.
Fisher College
Panelist

- 25 years in Industry Developing N-Tier Business Solutions
- Program Director and Professor at Fisher College in Boston
- Acting Program Director for New York University Cyber Fellows Program
- Research is in N-Tier and Cloud Application Correctness
During COVID, K-12 and Higher Education Moved to Cloud and Remote

• Society and news media have focused on challenges and failure
• I have experience with NYU and edX that show the opposite
• The quality of education including integrity and confidentiality have increased in these programs
• These are a model of the new economy that utilizes the cloud
NYU Cyber Fellows

- MS in Cyber Security
- 600 Students in First Two Years
- 100% Online
- Much Higher Quality than Brick and Mortar
- 75% Scholarship (75% Cheaper)
- Free Certificates to ensure students master prerequisites before first class
- Industry Partner Badges to master applied tooling
- NSA Cyber Operations and Cyber Defense
- CTF and Red/Blue Team Events with Industry
Certificates

Adult students may not have undergraduate classes, or they took them decades before. The certificates allow the students to master prerequisite content.

• Python
• C++
• Data Structures
• Discrete Math
edX MicroBachelors

• Online classes with labs and proctored exams offered by big name colleges.
• Credits Aggregated at one university (Thomas Edison)
• 1/3 cost of cheapest university
• NYU MicroBachelors Courses
Conclusions

• COVID and Cloud will change how we do business
• Integrity and confidentiality will be higher utilizing cloud and remote
• Old models were inefficient
System Operator: Managing Kubernetes Operators for Your System

Jiye Yu
Hitachi, Ltd. R&D Group
jiye.yu.kb@hitachi.com
Kubernetes Operators

**Issue:** It is infeasible for Kubernetes to manage thousands of applications with various working styles

- Kubernetes Operator is a solution
  - Concept Operator raised by CoreOS
  - Operator is designed for packaging, deploying and managing a Kubernetes application automatically

- How Kubernetes Operator works
  - Human operators who have deep knowledge on specific applications ‘teach’ Operators to repeat their work patterns on those applications.

- Benefits of Kubernetes Operator
  - Operators increase Kubernetes functionality
  - Make migration easier among various Kubernetes clusters
  - Ecosystem is growing – OperatorHub shares existing Operators to users
Consider a system consisting of two applications...

There is a system which is made of App1 and App2. The Operators are reconciling their own app respectively.

**Question**: As this is a system. Can we coordinate these two Operators as a whole?
Proposal of System Operator

Then, we tried to propose a concept of System Operator.

- It will be an Operator of the Operators.
What should System Operator do

• We designed System Operator’s features in three levels:
  
• Level1
  ✓ System construction, it looks like:
    
    ![System Construction Diagram](image)

  ✓ Operator’s update

• Level2
  ✓ System Monitoring
  ✓ Disaster recovery and regular backup

• Level3
  ✓ Auto-scaling to applications
How to achieve System Monitoring

Prometheus Operator will be a good bridge. Monitoring data is important for System Operator to do following system adjustment.
Summary and Future Work

System Operator allows users to

• Deploy system in Kubernetes by Operators
• Make global policy according to monitoring data
• Share your system by sharing the config of System Operator

System Operator is still under research

• We are considering more usecases for System Operator
• More features will be introduced into System Operator
Thank you!
“Cloud Technologies provide a huge diversity of services, but they lack IT-Security. Especially, with the growing amount of IoT devices, the security (and privacy) challenges are getting more and more...”

Sebastian Fischer (Fraunhofer AISEC, Germany)
Challenges

• Increasing services and amount of devices
• All-time accessible (cloud technologies)
• Cheap devices (especially IoT devices)
  • -> security risks
  • -> attack on a large scale
  • -> impact on privacy
Some Solutions

- Baseline requirements (security standards)
- Security awareness of the user
- Offline services
- Service free devices / Optional services
- What else???
IoT Security Standards

• Germany: DIN SPEC 27072 (Consumer IoT)
• Europe: ETSI EN 303 645 (Consumer IoT)
• US: NISTIR 8259 (Consumer IoT)
• IEC 62443 (Industrial IoT)
• …
Open Questions

- Current state of security
- The future of (cloud) services
- The future of IT-Security
- ...


The Complexities of Modern Cloud and the Impact on Compliance

Bob Duncan, University of Aberdeen, bobduncan@abdn.ac.uk

- Cloud security
- Corporate compliance
- Blockchain and the forensic trail
- Accountability

- IoT security is hard to balance due to complexity and untrained users
- Removing a need for centralized control of security is an opportunity for distributed systems
- Autonomous Systems require Autonomous Security
Outline

• Cloud Technologies
• Connected and Unconnected, yet Processing
• Cloud technological impact
• Service reliability
• Challenges
• Data and processes
• Trusted and secured environments
• Compliance with legislation and regulation
Cloud Technologies

- Cloud started as a simple suite of outsourced tools
- IaaS, PaaS or SaaS
- Service reliability was reasonable, security and privacy less so
- Now we have more things as a Service than can possibly fit on this page
- We can even have a cloud of clouds as a Service
- What started as three simple either/or options is now a mixture of combinations
- With included and excluded components, this equals more complexity
Connected and Unconnected, yet Processing

- Cloud can be permanently connected, and processing
- Cloud can be occasionally connected, and processing
- Cloud can incorporate remote processing of data
- Cloud can incorporate intermittent connections for data processing
- Cloud can do in-cloud processing
- Cloud can store in-cloud, or can use external storage
- Cloud can do connection by-request
- Cloud can do any permutation of these
Cloud technological impact

- Cloud offers rapid spooling up of new technology
- Cloud offers major reductions in capital investment requirements
- Cloud can offer major reductions in the need for large premises
- Cloud can offer high flexibility in change for new markets
- Cloud offers fast expanding startups the ability to complete with global corporates
Service reliability

• Service reliability was the initial major selling point for cloud
• That is still high, where one service provider is delivering the service
• When multiple service companies are involved, this can be compromised
• This can lead to slackness in some service providers “It wasn’t my fault, it was these other companies who did not …”
• On the plus side, those offering poor service tend not to be in business for long
• On the other hand, if you are relying on their service and get poor reliability….
Challenges

• Dealing with the complexities on offer can be challenging
• Coping with multiple service providers can lead to issues
• Ensuring proper security and privacy can still be a challenge
• Proper accountability where multiple service providers are involved
• Keeping track of data collected can be a problem
• The more complex your setup is, the more challenges you have
Data and processes

- Data is at the core of compliance with legislation and regulation
- Once multiple service providers are involved, this needs proper control
- With non-permanent connections, keeping proper track of the data is hard
- Keeping track of processes that are both in-cloud and external is also hard
- The more complexity that is possible = the more challenging it all becomes
Trusted and secured environments

- Large service providers are usually very ‘switched on’ on as far as trust and security are concerned, typically less so for smaller service providers
- Usually very well documented in the service level agreement
- They must be accountable for their actions, without ‘get-out’ clauses in the service level agreements
- Again, this is fundamental to the ability for the cloud user to achieve compliance with the relevant legislation and regulation
Compliance with legislation and regulation

• Cloud users are accountable to the legislative and regulatory authorities for ensuring they can demonstrate compliance
• Cloud users cannot ‘pass the buck’ to service providers as an excuse for any failures or shortcomings
• Using a complex cloud service structure could make compliance far less transparent, which can lead to issues with the regulators
• Cloud users who get it wrong are likely to face punitive action by the regulators, especially if they are negligent
Distributed security for distributed architectures:
Towards a blockchain enforced security model

Presentation is loosely based on the following paper:

Magnus Westerlund, DSc.
Principal Lecturer
magnus (dot) westerlund (at) arcada (dot) fi
Arcada University of Applied Sciences, Helsinki, Finland
Agenda

1. Introduction of Blockchain
2. What is blockchain useful for
3. Use Case: Security in IoT systems
4. Towards operationally autonomous security
What is Blockchain?

• A peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable, and updated by consensus among peer nodes.

• This provides useful technology for:
  – Finance, legal, logistics, e-currency/value tokens, security, and any business that is dependent on transactions between parties.

• Blockchain also introduces challenges for legal systems, companies preferring data silos, and traditional monetary/power systems.
Example use cases (beyond finance)

- Media, e.g. IPR, advertisement and subscriptions
- Computer/IoT security, the Internet was not constructed with security in mind, now a redo?
- Supply chain, globalization has led to increasingly complex supply chains, a decentralized platform can be an intermediary.

Most use cases focus on how to create a value-based economy for specific cases.

- The difference to the GOFA platforms is that now we do not need a trusted intermediary.
- The ledger provides global near instant transaction verification and a conceptually decentralized platform.
What is so different with blockchain solutions?

Image credit: Chris Umbach
Blockchain and DLT

• Distributed Ledger Technology (DLT)
  – DLT can include other technical implementations than block-based
  – Blockchain refers to early chains such as Bitcoin and Ethereum, that bundle transactions into blocks shared by peers (Fig 1).
  – DLTs include **distributed acyclic graphs**, for linking transactions and allows much faster throughput (Fig 3).

![Diagram](image_credit.png)

**Fig. 1.** Blockchain as a data structure.

**Fig. 3.** Transaction handling in the block lattice. S represents a *send* transaction, R represents a *recv* transaction.

Image credit: Bencic and Zarko arXiv:1804.10013v1
# Blockchain Evolution

<table>
<thead>
<tr>
<th>Generation</th>
<th>Innovation</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Distributed Ledger</td>
<td>Enforce a global “truth”, Bitcoin</td>
</tr>
<tr>
<td>2</td>
<td>Smart Contracts</td>
<td>Arbitrary transactions verified on-chain, Ethereum</td>
</tr>
<tr>
<td>3</td>
<td>De-facto standards for improved utility</td>
<td>Interledger transfers, reduction of transaction costs, and increased throughput, e.g. IOTA and Polkadot</td>
</tr>
</tbody>
</table>
What is an IoT system, today and in the future

• **Today**, reading data from sensors and acting through actuators
• **Tomorrow**, autonomous intelligent systems
• What we mean with an autonomous system is still unclear
  – One perspective is that they should be operationally autonomous
  – What is operationally autonomous security, should security not be under centralized control?
  – But how do we maintain a cryptographic setup for an autonomous system that is based on a distributed architecture?
  – Who maintains the keys?
  – How do we ensure devices are not breached?
  – How to ensure provenance and enable forensic investigations?
Security in IoT systems

• IoT security is a current large-scale problem that we must address
  – Current security is often based on trust for a centralized authority

• It is hard and costly to maintain IoT systems using traditional approaches, due to the nature of IoT systems:
  – distributed,
  – heterogeneous,
  – energy conserving,
  – plug and play,
  – limited computational power and storage

• Given the challenges, can we distribute the control of security?
An autonomous system should be self-contained

- Hardening the device in order to remove the ability to directly interact with it remotely, thereby reducing attack vectors
- The hypothesis is that all systems are breakable, but that we can make it “very hard” for anyone to get in.
  - Remove user log-in on the device, retain a system (OS) user.
  - Deny any externally initiated incoming connections to the device
  - Encrypt hard drive with system user credentials
  - Maintain a cryptographic protocol on the device that generates new keys for new data reporting tasks
Push-pull communication method

- Going towards autonomous systems means they should maintain themselves and deal with security by themselves.
  - Let us rely on the blockchain for a ground truth of how a well-maintained system should look like
  - Let us maintain any licenses needed on the blockchain
  - Devices should only perform externally initiated operations based on a push-pull method
  - Thus, commands are not sent directly to devices, but rather through the blockchain that the device fetches.
Smart Contracts defines the security protocol

- Through smart contracts we can implement arbitrary transactions
- Here we define User and Device and their respective properties
- Initially the user links themselves and the device to the blockchain by creating a unique Ethereum address.
- Then the user links both to the respective smart contracts

Executing a task on the device

• Let us consider a trivial task were a user wants to measure the temperature of the environment that the device reside in without directly controlling the device or a centralized API that controls the device
  – Then User (Creator) purchase tokens, and uses these to Add a task
  – A Device receives the Task, accepts it by providing a stake
  – Device takes the measurement and completes the Task by returning the measurement to an endpoint the Creator provided
  – The stake and the token Fee is returned to the Device or device Owner contract

Summary

• The proposed protocol can be used for creating operationally autonomous IoT devices, i.e. self-contained.

• The device can still perform advanced and arbitrary tasks
  – We are currently working on implementing a service layer

• The hardening will make it very hard for an intruder to attack

• We can create an economy around IoT services and security that have previously not been possible
  – E.g. very easy to provide a per instance payment for a security patch

• Easy to also implement for your own chain if needed
  – Less reliable than using Ethereum, but lower overhead cost per transaction
Thank you!

Magnus Westerlund, DSc.
magnus.westerlund@arcada.fi