SECURED EDGE INFRASTRUCTURE FOR CONTACTLESS PAYMENT SYSTEM

A case study on EV charging solution based on StarlingX

Zu lijun, UnionPay
Sun, Yih Leung, Intel DCG
Wang Haitao, Intel IAGS/SSP

Intel
Legal Notices and Disclaimers

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest forecast, schedule, specifications and roadmaps.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request. No product or component can be absolutely secure.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

Intel, the Intel logo, Pentium, Celeron, Atom, Core, Xeon, Movidius and others are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

© 2019 Intel Corporation.
The value of edge computing for finance

- The core focus of finance—risk controllable
- The value of edge computing in reducing risk
  - Data
    Because it is close to the information source, it can obtain real-time, complete and real information, and the information is difficult to be tampered with. This is the value of the traditional POS. Through this information, the scene of the transaction can be clarified, and the transaction type can be accurately located.
  - Privacy
    The filtering of sensitive data is completed on the edge of the network, and the privacy information other than the payment service requirement is removed. For example, when performing face recognition payment, the edge computing node converts the face image into an adult face feature, and only submits the face feature to the payment background. It does not submit face images, which protects users’ personal information and reduces risk.
Edge computing financial solutions in car charging scenarios

- Connect the charging vehicle to the edge computing gateway via a wired device (such as a power line) to directly obtain vehicle information and use the vehicle information as a payment marker.

- **Replace the industrial computer with an edge computing gateway, significantly reducing costs**

- The payment control is integrated in the edge computing gateway, and the order is initiated directly from the gateway, which clarifies the real trading scenario of the order.

- Edge computing gateway integrates IoT security chip to provide financial-grade hardware security hardening solution to improve data reliability.

- Joint business department to design a non-inductive payment interface for car charging payment, and use the vehicle VIN number to pay for the gun to pay and improve the user experience.
Non-inductive charging payment architecture based on edge computing gateway

Cloud

Industrial and family edge

On site

UnionPay (Internet of Things Payment Platform)

Acquiring institution (Non-inductive payment platform)

Charging operation platform

Charging pile

Car owner

Charging vehicle

Security service

Management service

Payment entry

Payment service

Payment entry

Payment service
Edge Computing Gateway - POS in the Internet of Things

**Support for multiple protocols**
The edge computing gateway should support the protocol running on the underlying physical device so that it can read the information content transmitted by the physical device.

**Payment function**
Empower the edge calculation node so that the location of the generated order is close to where the transaction occurred, ensuring that the order is authentic.

**Location and time service**
Provide accurate location and time information for financial services, make transactions more authentic and reliable, and effectively avoid illegal operations such as transfer.

**Communication function**
Flexible network access, multi-scenario support, reliable data transmission capability in the IoT environment.

**Security service**
Financial-grade encryption provides support for data security and trustworthiness; system-level security protection protects itself from physical and cyber attacks.

**Hardware constraints**
Adapt to a variety of application scenarios, can work reliably and stably in harsh environments.

**Edge computing gateway software**
- No sense payment control
- Security hardening
- Management interface
- Internet of Things Communication Protocol
- Standard charging pile agreement
- Location service
- Time service
- Communication service

**Edge computing gateway hardware**
- GPS
- 4G/5G
- Ethernet port
- Internet of Things Security Chip
- CPU
- RAM
- hard disk

Financial-grade encryption provides support for data security and trustworthiness; system-level security protection protects itself from physical and cyber attacks.

Adapt to a variety of application scenarios, can work reliably and stably in harsh environments.
Security reinforcement for edge calculation

- **Traditional gateway**
  Traditional gateways tend to focus on data forwarding, lacking sufficient attention in security and making it difficult to undertake financial services.

- **Gateway under financial business**
  Due to the empowerment of financial services, the security of gateways becomes more and more important, and stricter requirements are imposed on security hardening.
  - Trusted Execution Environment (TEE)
  - Blockchain Service Network (National Information Center, China UnionPay, China Mobile)
  - Financial Security Chip from UnionPay
The structure of UnionPay’s edge computing management platform

Well-built platform capabilities

Cross-industry equipment access

It can access payment gateways in different industries and be integrated into the platform for unified management.

Remote monitoring operation and maintenance

The cloud visualizes the local physical device and supports remote access to the device console and file system for operation and maintenance.

Edge intelligence

Support local AI through the edge AI framework to provide multiple value-added services in addition to payment.

Cloud and edge integration

The cloud configures and manages the calculation rules and local business applications, which are synchronized to the edge gateway through the deployment function and run automatically.
SECURITY INFRASTRUCTURE FOR CONTACTLESS PAYMENT

- Security is a must-have
- Security system engineering is dynamic
- Security comes at a cost

- StarlingX is a fully open sourced, industry leading software platform, optimized for edge computing and designed for edge deployments.
- StarlingX provides a reference stack for security infrastructure for contactless payment, to accelerate the go-to-market and ease of edge deployments for this emerging business opportunities.

StarlingX is your choice for open infrastructure for security

* Other names and brands may be claimed as the property of others.
SOFTWARE ARCHITECTURE RECAP

StarlingX
- Virtualized Infrastructure Manager
- Infrastructure Orchestration

OpenStack
- Host Management
- Configuration Management
- Fault Management
- Software Management
- Service Management

Kubernetes
- Helm
- Armada
- Docker Registry

Virtualized Infrastructure Manager
- IPMI
- TPM
- HTTPS
- Apache
- Ceph
- Postgresql
- Etc
- etc
- Calico
- NGINX
- OvS
- KVM
- EMU

Hardened Linux

Hosted Virtualized Applications
- Any Guest OS
- Canonical
- VxWorks
- Redhat

Infrastructure Orchestration
- Fault Management
- Host Management

COMMUNITY OF SECURITY FEATURE PORTFOLIO

Host environment
- UEFI secure boot and signed images
- User and group permissions
- Virtual TPM for secure guests

AAA
- Network firewall on external OAM interface
- Role-based access control
- External LDAP integration via Keystone

Integrity
- Critical process monitoring and recovery
- Resource monitoring on Control nodes
- Tenant data stored on private network

Confidentiality
- Management network encryption
- Secure keyring database for storage of encrypted passwords
- QoS for protection of connectivity to hosted VMs
- TLS security & TPM certificate storage

* Other names and brands may be claimed as the property of others.

Thank you to the employers of Contributors to the 1.0 Release

https://www.starlingx.io/supporters/
EV CHARGING EDGE WORKLOAD CONSOLIDATION

- **Way of Payment Is Changing**
  - Contactless payment in EV charging station, by combining vehicle SN and personal bank account

- **Customer Pain Points**
  - Secure and unsecure workload isolation
  - Scalability, easy deployment and maintenance by workload consolidation from client to edge

* Other names and brands may be claimed as the property of others.
Car plate detection when a valid e-vehicle is parking - A security-enhanced use case
SYNERGY TO DATA ANALYTIC USE CASE

Analytic based on big data collected at edge - A security-enhanced use case

* Other names and brands may be claimed as the property of others.
### Stack for Open Infrastructure in Security Perspective

#### Security Development Lifecycle

<table>
<thead>
<tr>
<th>Security</th>
<th>User Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Frameworks: Spark, TensorFlow/Pytorch, OpenVINO, AnalyticZoo</td>
</tr>
<tr>
<td></td>
<td>Orchestration: OpenStack, SDN, SDS, K8s, StarlingX</td>
</tr>
<tr>
<td></td>
<td>Hypervisor: KVM, ACRN, Kata Container</td>
</tr>
<tr>
<td></td>
<td>OS: CentOS, OpenSUSE, Ubuntu</td>
</tr>
<tr>
<td></td>
<td>OneAPI</td>
</tr>
<tr>
<td></td>
<td>Firmware/BIOS UEFI</td>
</tr>
</tbody>
</table>

#### Connectivity
- Ethernet, 5G/4G, WIFI/BT GPS

#### Storage
- Hard disk
- Flash AeP

#### Security MVP:
- {TEE:SGX, VM}
- {secure boot}
- {secure storage: PTT/PTM}
- {PKI Device ID}
- {Crypto: HW accelerated}
- {FIPS 140-2}
- {HW security}

#### Community Customer Co-engineering

<table>
<thead>
<tr>
<th>Retail</th>
<th>Industrial</th>
<th>DSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Manageability Provisioning Recovery Predictive analysis vPro AMT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provisioning and LCM Network protection and attestation SW orchestration, SDIS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple RoT w/ FPGA/Moveidus Encrypted video streams Video watermarks Provisioning</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Open Community of StarlingX extends stack portfolio

Ref: S.Cheruvi et al. Demystifying Internet of Things Security, 2019

* Other names and brands may be claimed as the property of others.
CONCLUSION

• Open Source software platform from cloud to edge
• Open Design for future proof infrastructure optimized for security
• Open Development for security hardening
• Open Community ecosystem to security feature portfolio

Welcome to visit our StarlingX demo booth

* Other names and brands may be claimed as the property of others.
A Fully Featured Cloud For The Distributed Edge

Join the Community

Mailing Lists: lists.starlingx.io
Freenode IRC: #starlingx
Website: www.starlingx.io

Join the Foundation mailing list to stay up to date on all new projects!

http://lists.openstack.org/cgi-bin/mailman/listinfo/foundation