



Huawei Kunpeng Computing Web Application Solution



Contents

1. Web Trends and Challenges
2. Huawei Kunpeng Computing Web Solution
3. Case Studies



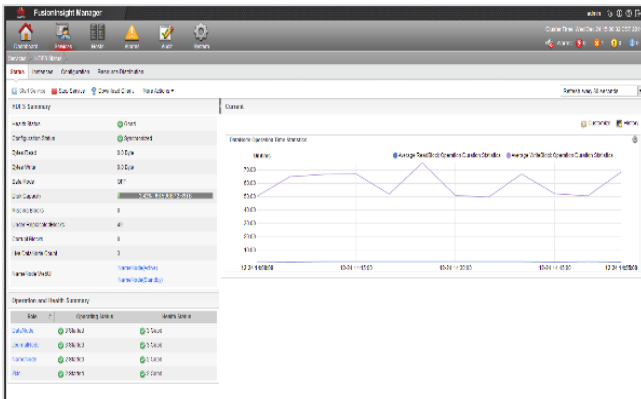
Typical Web Applications



Government information systems



Financial transaction and settlement systems



Carriers' billing and CRM systems

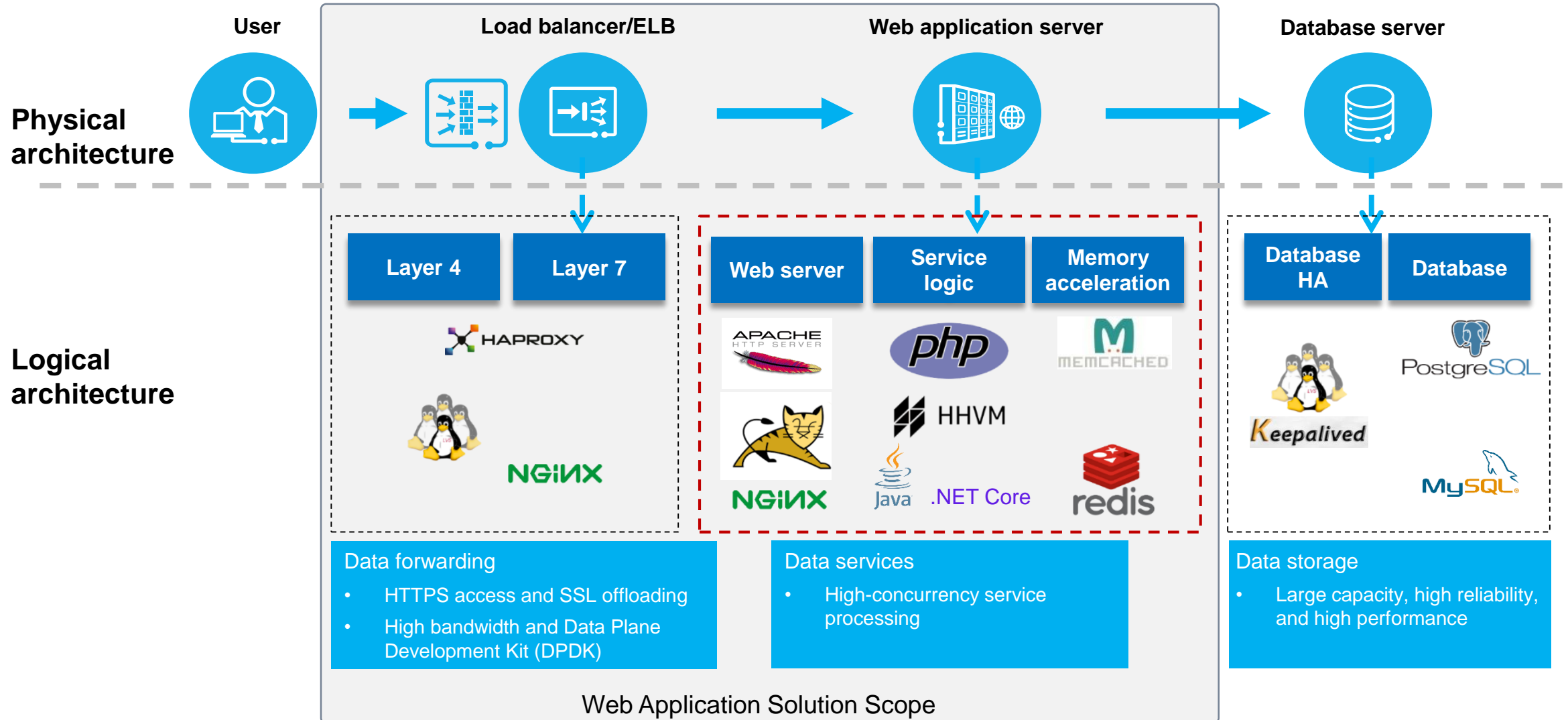


Other web applications

- Governments: government and department websites, general service platforms, and management systems
- Finance: bank websites, web application servers of channel transaction systems, and web middleware servers of settlement systems
- Carriers: web applications and middleware servers for systems such as O&M management, billing, and CRM
- Other: HTTPS-based SSL offloading, web load balancing, web servers, web cache, and more



Web Application Architecture

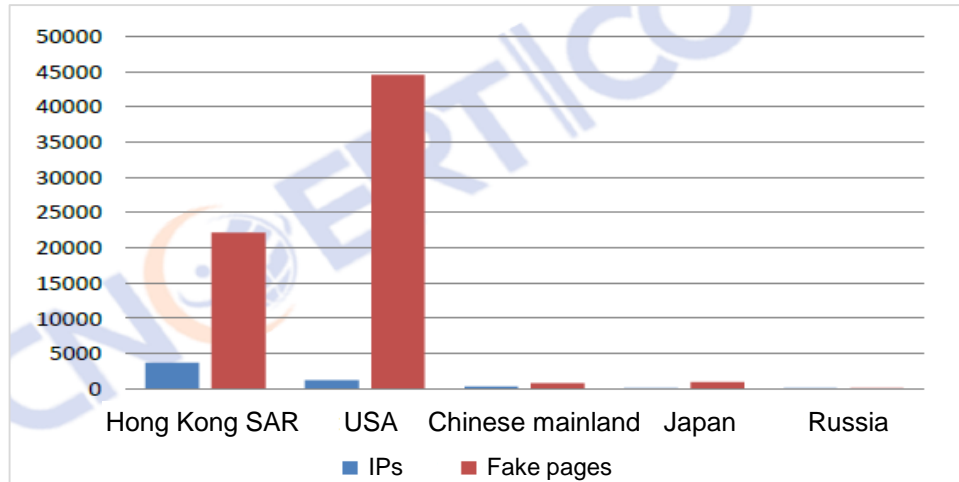




Security Challenges Faced by Web Applications

Fake web pages

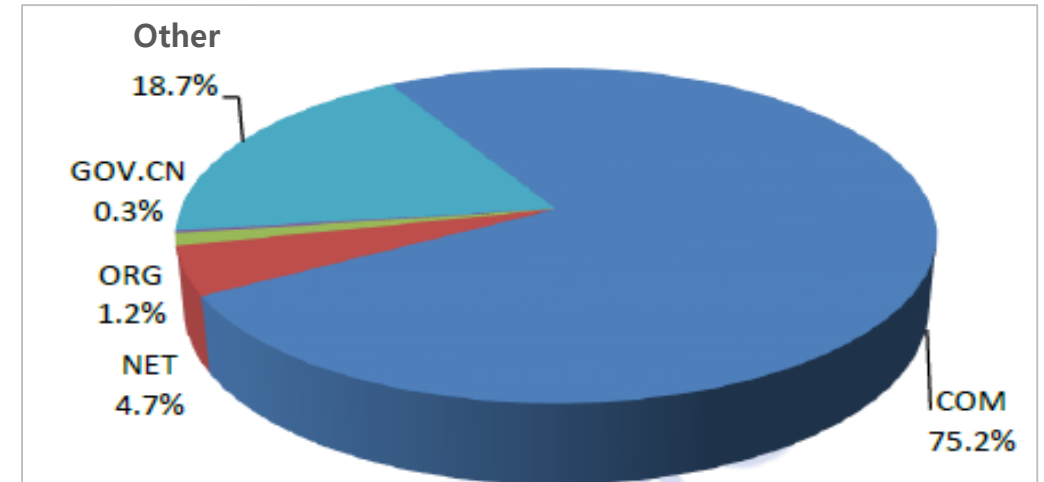
- In 2019, **85,000** fake pages were detected against Chinese websites, an increase of **59.7%** over 2018.
- The source IP addresses of those fake pages were mainly distributed **in the Hong Kong SAR (China) and the USA**, relating to financial and telecommunications industries.



Fake pages and their IP addresses in 2019

Web tamper

- In 2019, approximately **186,000** Chinese websites were tampered with, including **515** government websites.
- According to their domain name levels, .com, .net, and .org rank the top three, accounting for 75.2%, 4.7%, and 1.2% respectively.



Tampered websites in 2019

Data source: China's Internet Security Situation Summary Report for 2019, released by National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC)



HTTPS Chosen by Most Websites

More secure

- Data encryption and secure channels protect data during transmission.
- Identity authentication verifies the authenticity of websites.
- Data integrity prevents data from being forged or tampered with.

Hypertext Transfer Protocol Secure

Data transfer secured with SSL

Secure Sockets Layer

Secure protocol for network communication

Hypertext Transfer Protocol

Data transfer in plaintext with low security

HTTPS

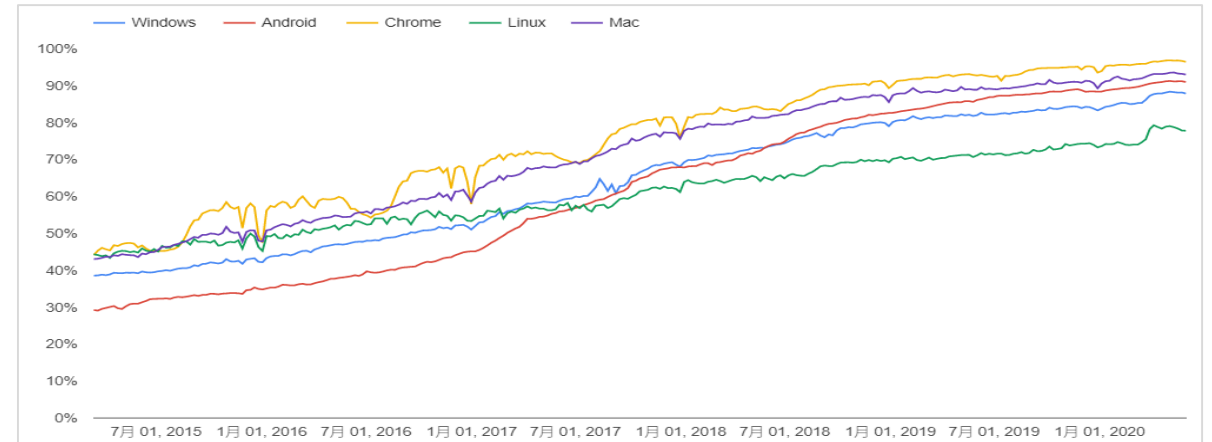
||

SSL

+

HTTP

Choice for mainstream browsers and websites



Platform-specific percentage of web pages loaded over HTTPS on Chrome

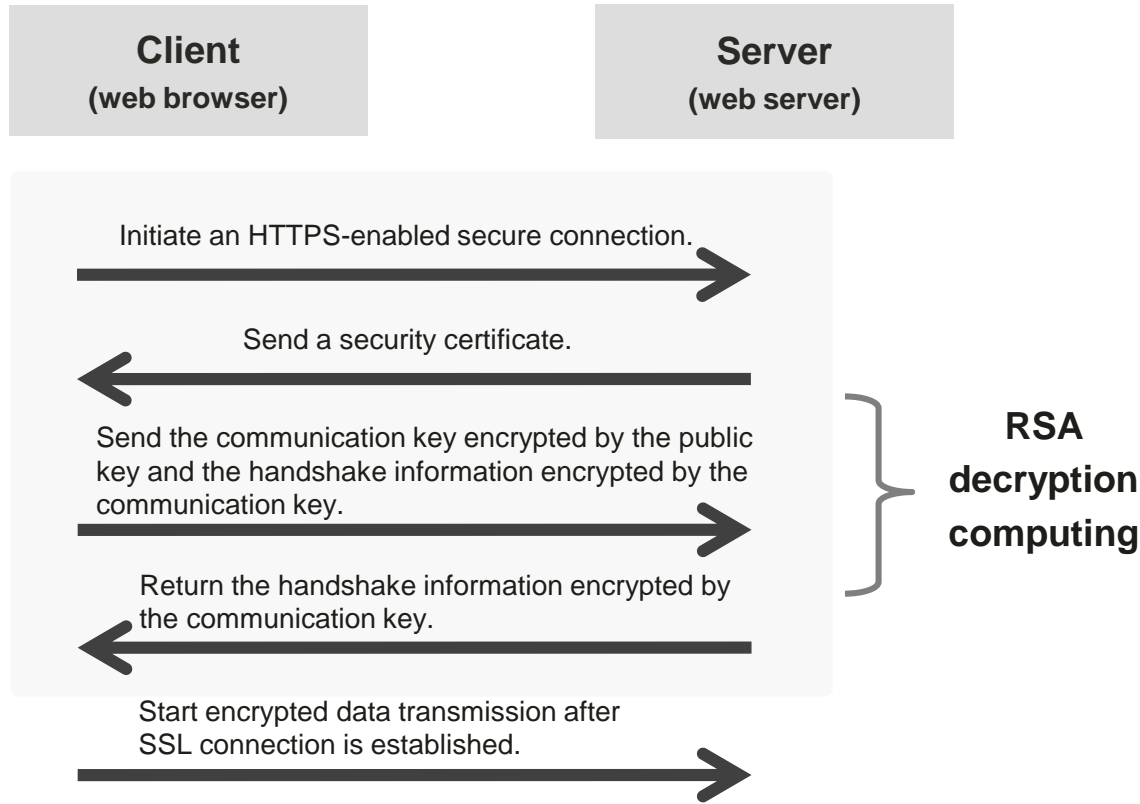
By May 30, 2020,

- On Windows: 88% of web pages use HTTPS.
- On Android: 91% of traffic goes through HTTPS.
- On Mac and Chrome: 93% and 96% network traffic is protected using HTTPS, respectively.
- Among the 100 most popular websites, 96 have enabled HTTPS onsite.

Data source: Google Transparency Report



Accelerating RSA Encryption and Decryption to Improve HTTPS Connection Performance



An HTTPS connection requires handshakes based on RSA encryption and decryption.

- Identity authentication and data key exchange
- Large amount of RSA-based asymmetric encryption and decryption

HTTPS Connection Types

Type	Description	Typical Scenario
Short connection	<ul style="list-style-type: none">• A TCP connection is established for each interaction, and is closed after data transmission is complete.• The RSA computing accounts for more than 20%, sometimes as high as 80% in extreme scenarios, of the time taken to process a short connection.	Web browsing websites
Persistent connection	<ul style="list-style-type: none">• Multiple data packets can be sent on a TCP connection. If the sending times out or the client proactively disconnects from the server, the TCP connection is closed.• The RSA computing accounts for 3% to 10% of the time taken to process a connection.	Chats and live video streaming

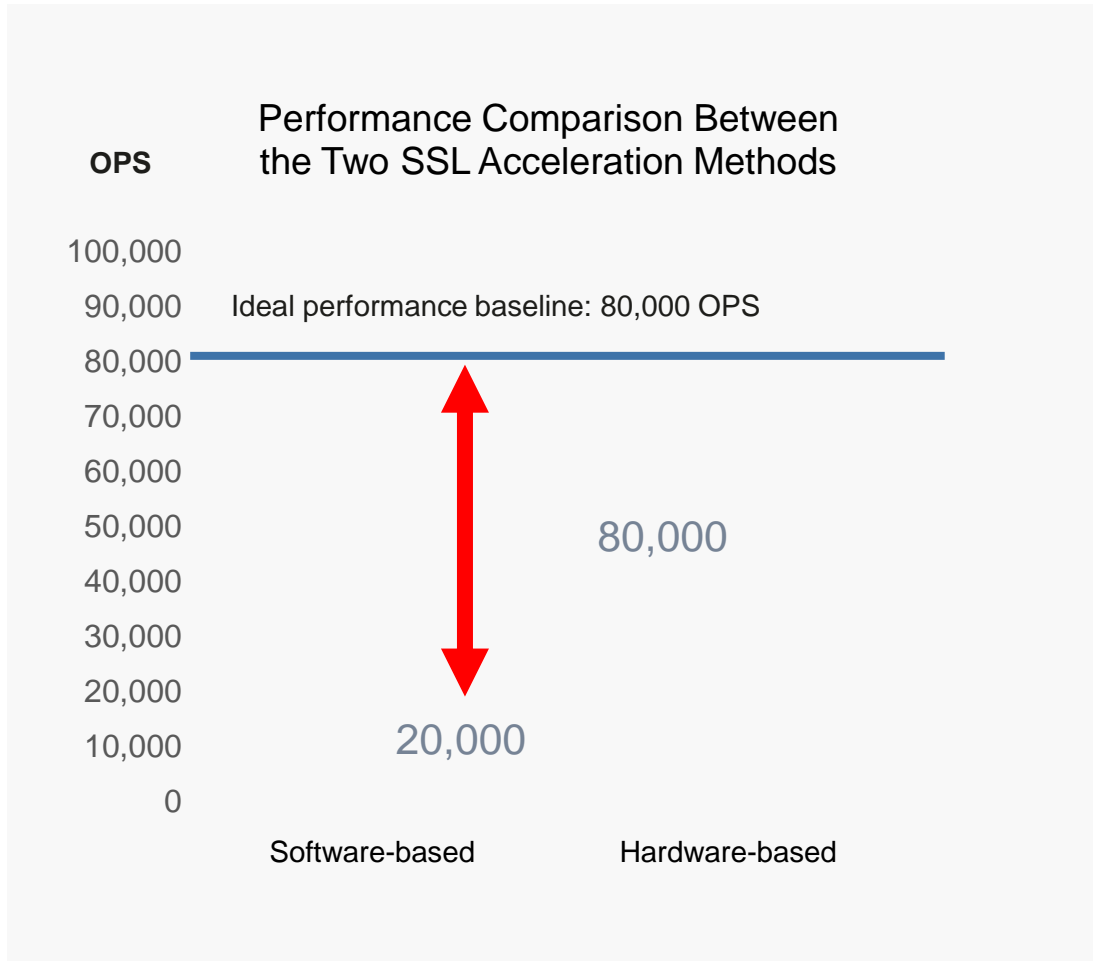
Remarks:

Short connection: Set up a connection -> Transmit data -> Close the connection ... Set up a connection -> Transmit data -> Close the connection

Persistent connection: Set up a connection -> Transmit data -> Keep the connection -> Transmit data -> -> Wait until one party closes the connection (in most cases the client does)



High-Performance and Efficient SSL Acceleration



Challenge 1: Software SSL acceleration performs poorly.

- **Inferior performance, only 20% to 25%** of the needed
- Deteriorated system performance since extra CPU resources are occupied

Challenge 2: Hardware SSL acceleration cards increase CAPEX.

- **Increased CAPEX**
- Server expansion resources occupied

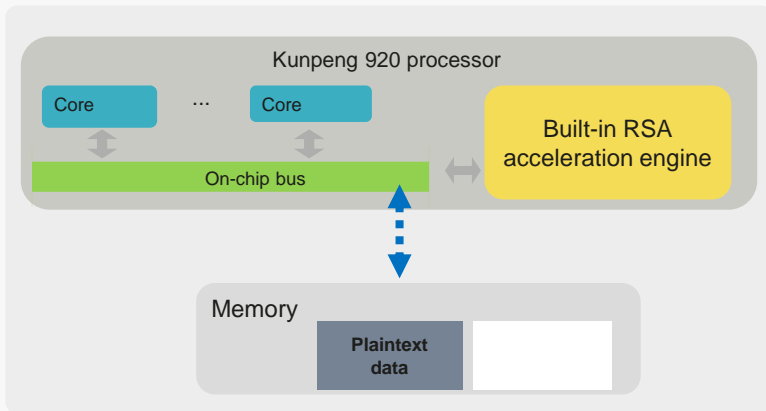
- Typical algorithm: RSA 2048, asymmetric data encryption.
- CPU soft computing: A typical 2-socket server provides a processing capability of **less than 20,000 times per second**.
- Hardware acceleration card: A single server can deliver a performance of 80,000 to 100,000 times per second.



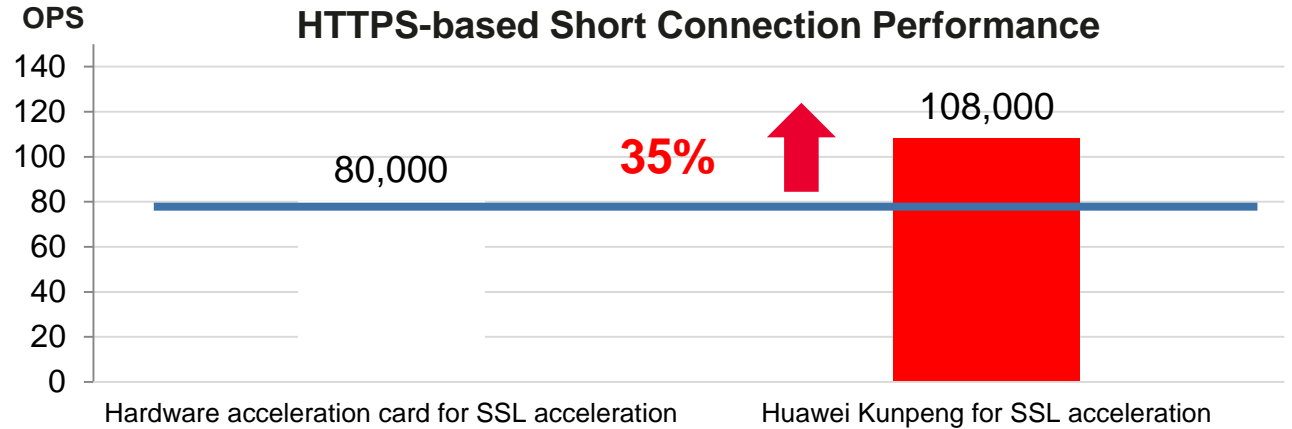
Kunpeng SSL Hardware Acceleration

35% higher RSA performance than hardware acceleration cards

Kunpeng processor with a built-in RSA acceleration engine



- The Kunpeng 920 processor has an RSA accelerator inside. The RSA 2048 performance reaches 50,000 OPS.
- A Kunpeng 2-socket server provides an RSA performance of 108,000 OPS, which is 35% higher than hardware acceleration cards.



Platform configuration

Traditional Hardware Platform

2 x CPUs + 2 x hardware acceleration cards

TaiShan 200 Server (Model: 2280)

2 x Kunpeng 920 5250
(built-in RSA acceleration engine)

CentOS 7.6

Tengine-2.2.2

httpress-1.1.0-2.el7.x86_64

Memory: 12 x 32 GB DDR4 2666 MHz

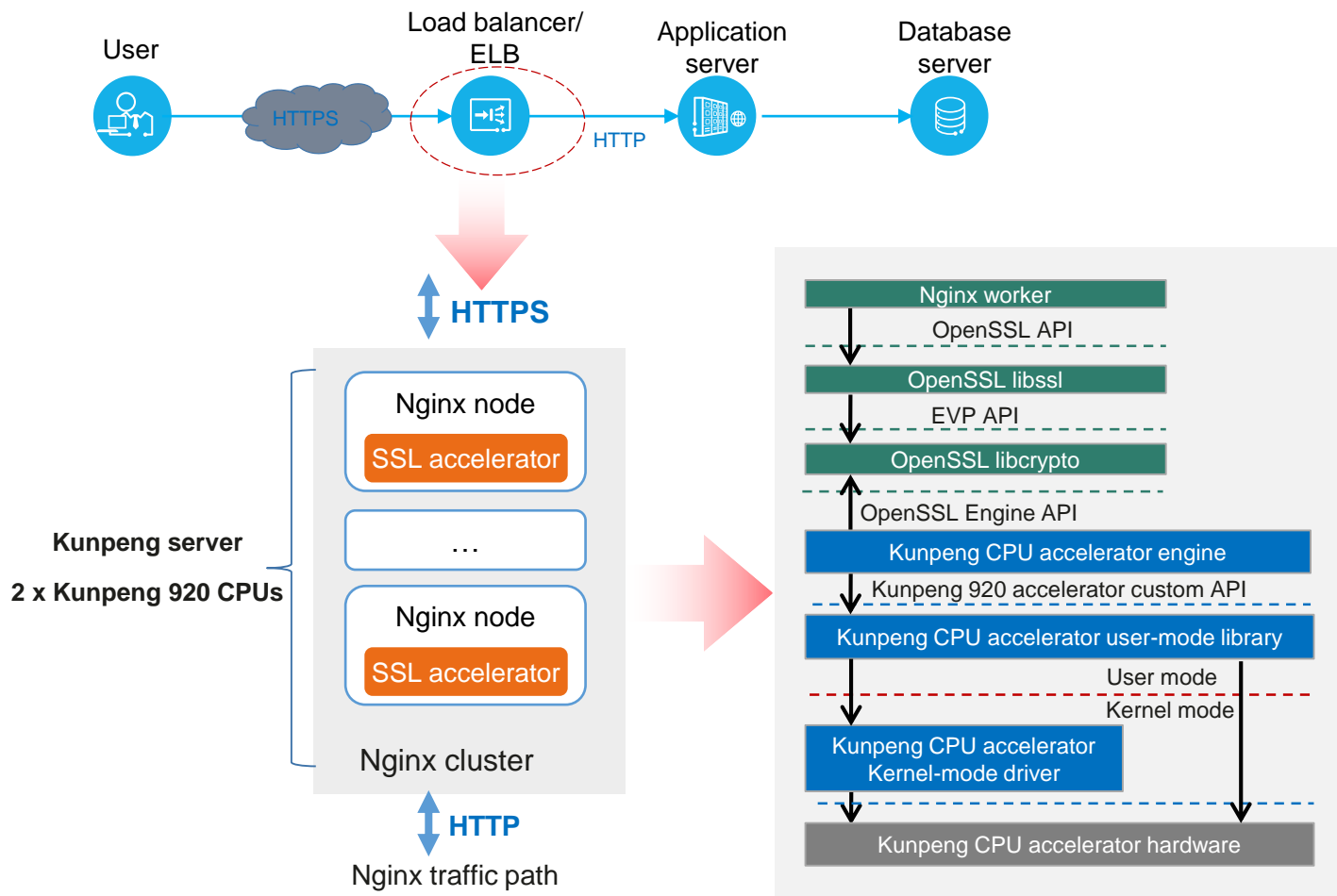
Data drive: 1 x 1.6 TB ES3000 V5 SSD

Data source: Huawei labs. A larger number indicates a higher performance.



Invoking Kunpeng SSL Acceleration

Process of invoking the Kunpeng RSA acceleration engine



How to Use

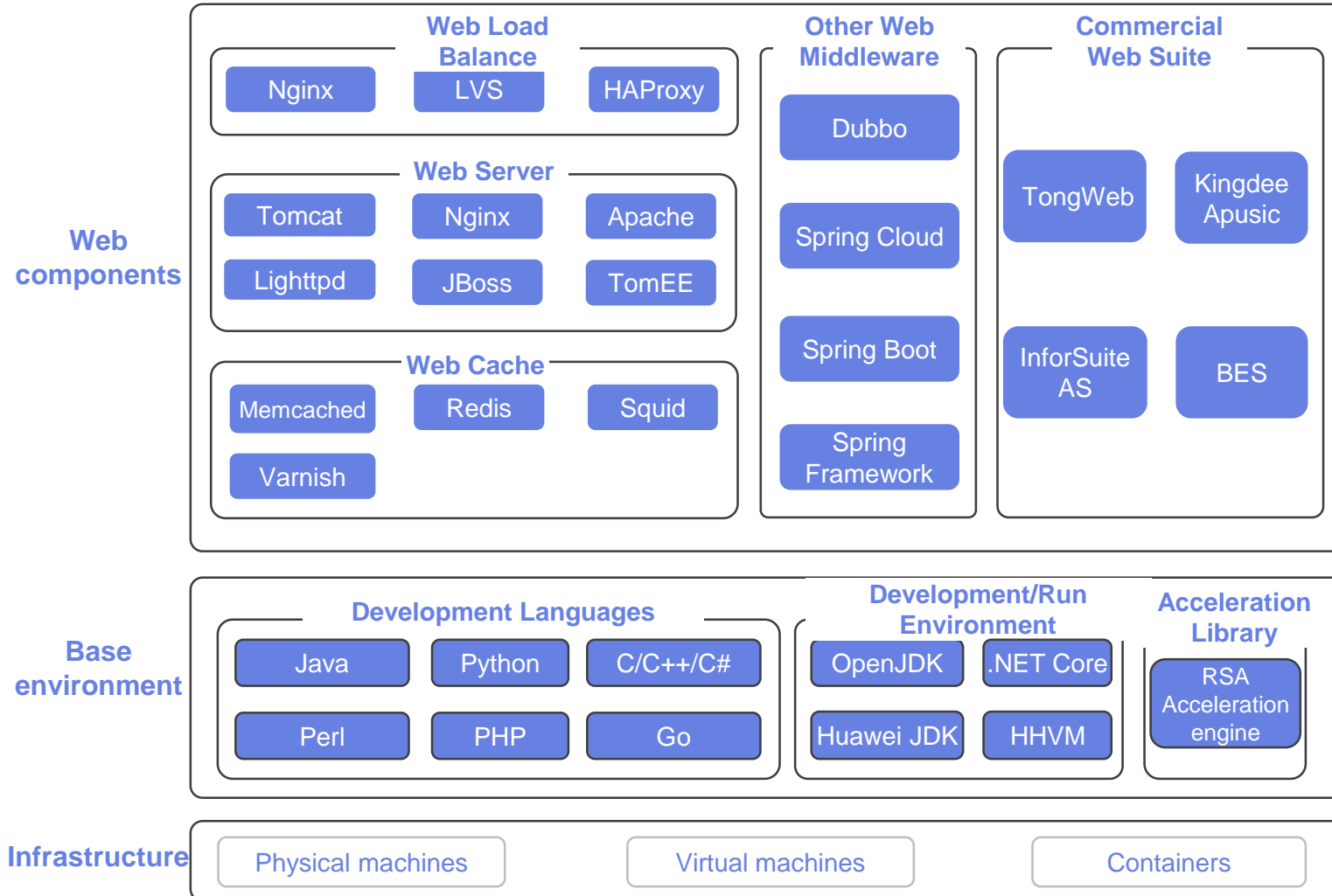
- ✓ Install the accelerator engine driver.
- ✓ Install the Nginx software (Tengine is recommended for its asynchronous mode).
- ✓ Configure the HTTPS digital certificate.
- ✓ Enable the Nginx asynchronous mode (`ssl_async` parameter).

Two types of APIs are available to invoking:

API	Description	Typical Application
OpenSSL APIs	The accelerator is integrated into OpenSSL as an engine.	Nginx, Tengine User-developed software
Custom APIs	User-mode library, available to be invoked by users' software	User-developed software



Kunpeng Computing Web Application Software Ecosystem

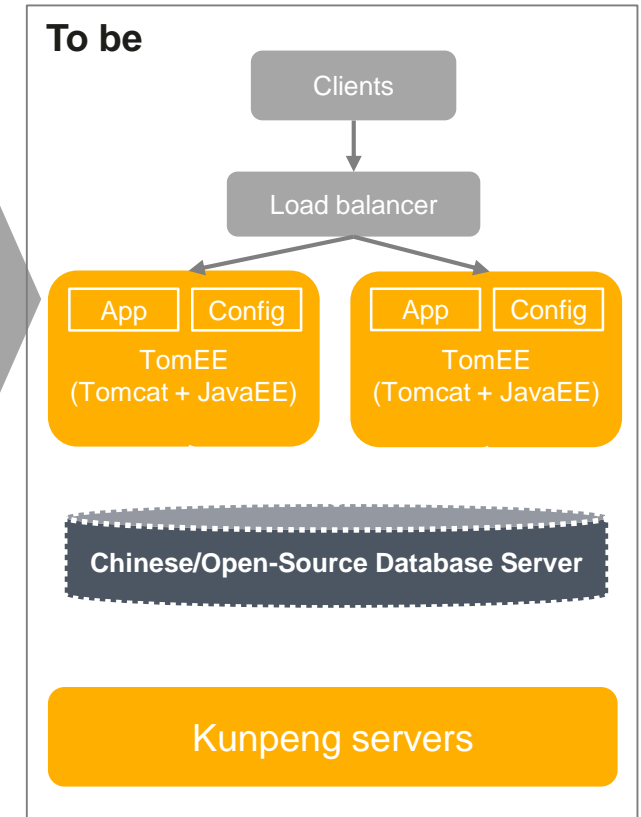
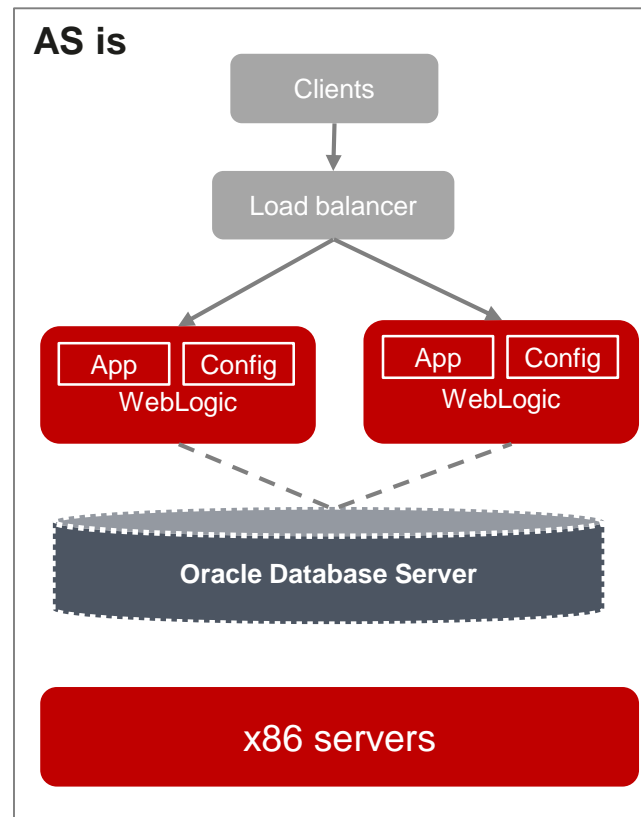
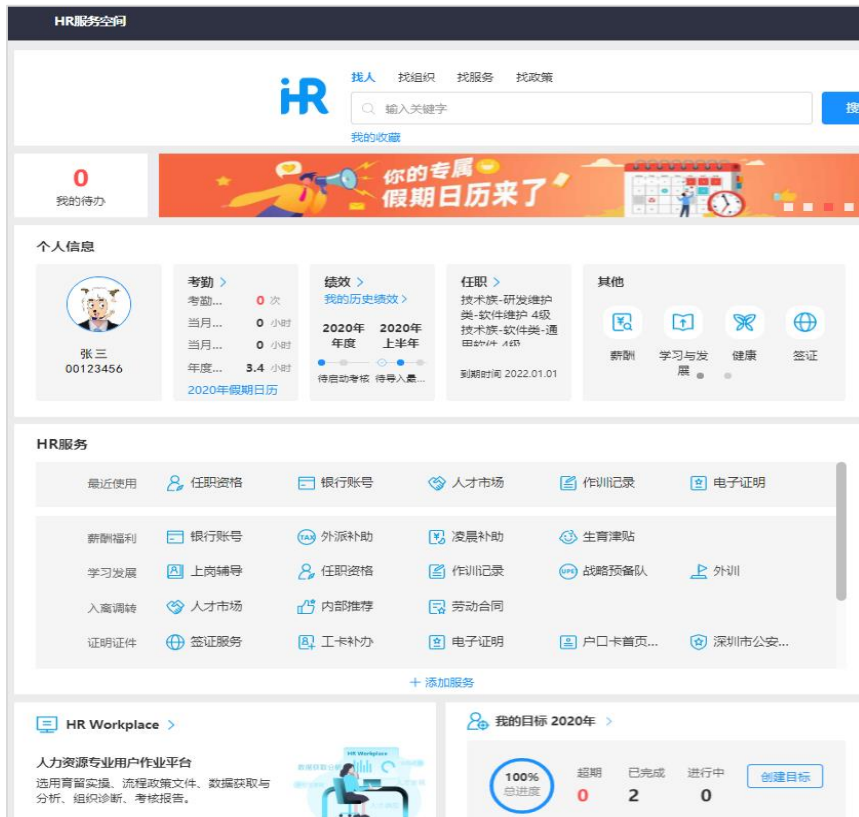


- Mainstream open-source middleware such as Nginx and Tomcat
- Mainstream middleware such as TongWeb, Kingdee Apusic, InforSuite AS, and BES
- Web applications and microservice application components such as Dubbo, Spring Cloud, Spring Boot, and Spring Framework
- .NET Core framework, with support for porting applications from .NET Framework
- TomEE, with support for porting applications from WebLogic and WebSphere



Porting from WebLogic to TomEE

WCAPortal application in Huawei's internal HR system



- Huawei's internal HR application was developed on the WebLogic-based ADF framework using Oracle JDeveloper IDE, and was deployed on x86 servers.
- Use Kunpeng servers and TomEE to replace the x86 servers and WebLogic. After the porting is complete, the applications continue to run properly.



Summary: Why Choose Kunpeng for Web Servers?

- **High performance:**

Built-in RSA acceleration engine: SSL offloading supported, 35% higher performance than hardware acceleration cards

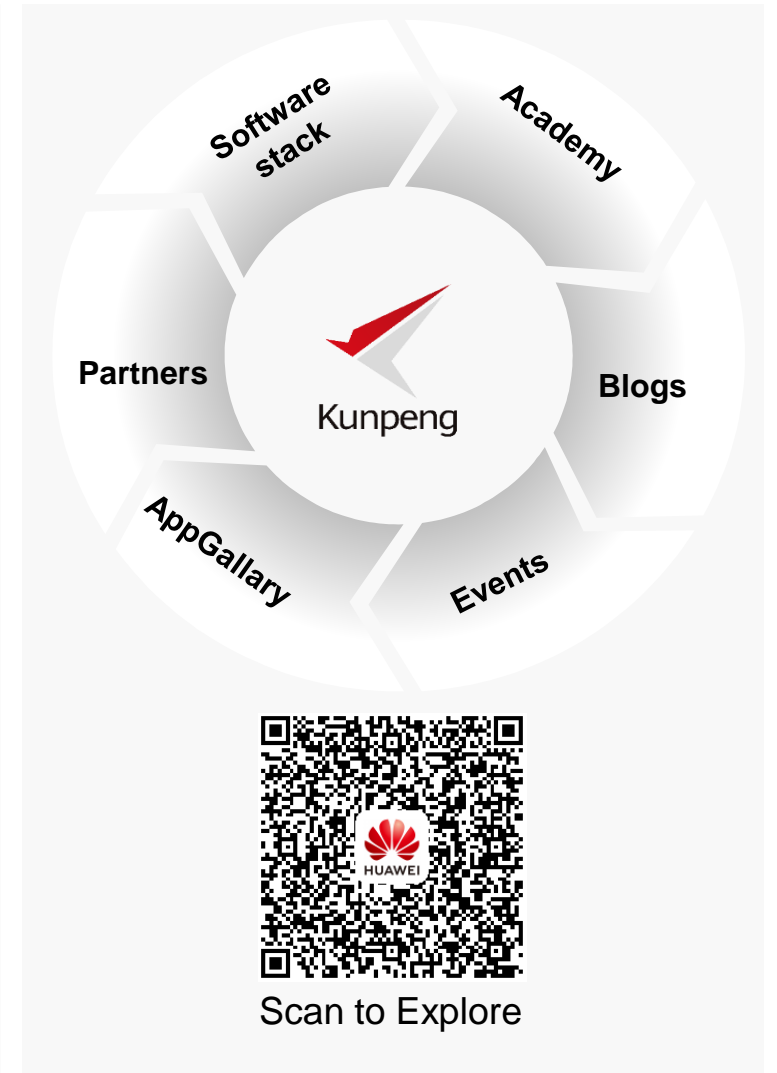
- **Rich ecosystem:**

Wide compatibility with open-source web software and China home-made commercial software



More About Web Applications

Available At	Document Name	Link
Kunpeng Community	Technical White Paper	https://support.huaweicloud.com/twp-kunpengwebs/kunpengwebs_19_0002.html
	Feature List	https://support.huaweicloud.com/twp-kunpengwebs/kunpengwebs_19_0014.html
	Porting Guide	https://support.huaweicloud.com/prtg-kunpengwebs/kunpengnix_02_0001.html
	Deployment Guide	https://support.huaweicloud.com/dpmg-kunpengwebs/kunpengnix_04_0001.html
	Tuning Guide	https://support.huaweicloud.com/tngg-kunpengwebs/kunpengnix_05_0002.html
	Porting Guide	https://bbs.huaweicloud.com/forum/forum.php?mod=forumdisplay&fid=931&orderby=lastpost&filter=typeid&typeid=824&orderby=lastpost





Thank You.

Copyright © 2021 Huawei Technologies Co., Ltd. All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

Grow With Intelligence