

Performance and Security

in IoT

Team Emertxe



Performance and Security

Benchmarking



A method to measure the performance of a product with another which is considered to be the best in the industry



Performance and Security

Benchmarking - General Steps



- Choose a product, service to benchmark
- Determine which best-in-class cloud provider you should benchmark against
- Gather information on their internal performance, or metrics
- Compare the data from both providers to identify gaps in your choice



Performance and Security

What to Benchmark?

- Sets of services
- Target market
- Business models
- Customer base etc.,



Performance and Security

Benchmark based on Reference Model



- Data and connectivity management
 - Device discovery, authentication, management and control
- Context-awareness
 - Collecting, managing and using contextual information (event processing for example)
- Scalability
 - Being able to enlarge the deployment of devices, agnostically from the type of devices (importance of drivers and APIs)
- Security
 - Ensuring the security, the privacy and the integrity of the data gathered



Performance and Security

Benchmark based on Reference Model



- Data analytics and visualization tools
 - Being able to analyse different data sources (big versus low data, real-time versus batches, high velocity of data production versus low velocity)
- Interoperability
 - Being flexible enough to engage with other software solutions and exogenous data sources (IT data for example)
- Innovation enabler
 - Creating ecosystem of users and developers through application enablement suites



Performance and Security

MQTT vs HTTP



Criteria	MQTT	HTTP
Architecture	Publish/Subscribe	Request/Response
Header Size	2 Byte	Undefined
Message size	Small and Undefined (up to 256 MB maximum size)	Large and Undefined (depends on the web server or the programming technology)
Semantics/ Methods	Connect, Disconnect, Publish, Subscribe, Unsubscribe, Close	Get, Post, Head, Put, Patch, Options, Connect, Delete
Quality of Service (QoS) /Reliability	QoS 0 - At most once QoS 1 - At least once QoS 2 - Exactly once	Limited (via Transport Protocol - TCP)
Transport Protocol	TCP (MQTT-SN can use UDP)	TCP
Security	TLS/SSL	TLS/SSL
Default Port	1883/8883 (TLS/SSL)	80/443 (TLS/SSL)



Performance and Security

MQTT vs HTTP Performance



- <https://cloud.google.com/blog/products/iot-devices/http-vs-mqtt-a-tale-of-two-iot-protocols>
- <https://flespi.com/blog/http-vs-mqtt-performance-tests>



Performance and Security

Security - Threat

- Cloning of things
- Substitution
- Eavesdropping / Man-in-the-middle
- Privacy
- Denial-of-Service
- Firmware replacement
- Routing attacks



Performance and Security

Security - Challenges



- Device heterogeneity
- Protocol translation vs. end-to-end security
- Software update
- Verifying device behavior
- End-of-life
- Penetration testing
- Quantum resistance



Performance and Security

Security - Consideration



- Researching the reputation of the vendor and solution, including reviewing security notices
- Implementing a secure, isolated network environment for IoT systems separate from other networked systems
- Setting strong, unique passwords for IoT interfaces providing time services
- Enabling multi-factor authentication if possible
- Selecting IoT solutions that provide a centralized management interface for managing passwords, configurations and firmware updates
- Hardening devices by changing default settings to the most secure option following vendor instructions, provide regular patches and upgrades



Performance and Security

Security - Firmware Upgrade



- As we all know the internet of thing (as the name implies) is always connected to network, there are susceptible to external attacks
- These attacks are generally carried overs by exploiting the bugs available in the software
- So constant checks on the running system, and increase its security feature plays an important role



Performance and Security

Cryptography



Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries

Source: Wiki



Performance and Security

Cryptography - Primary Functions



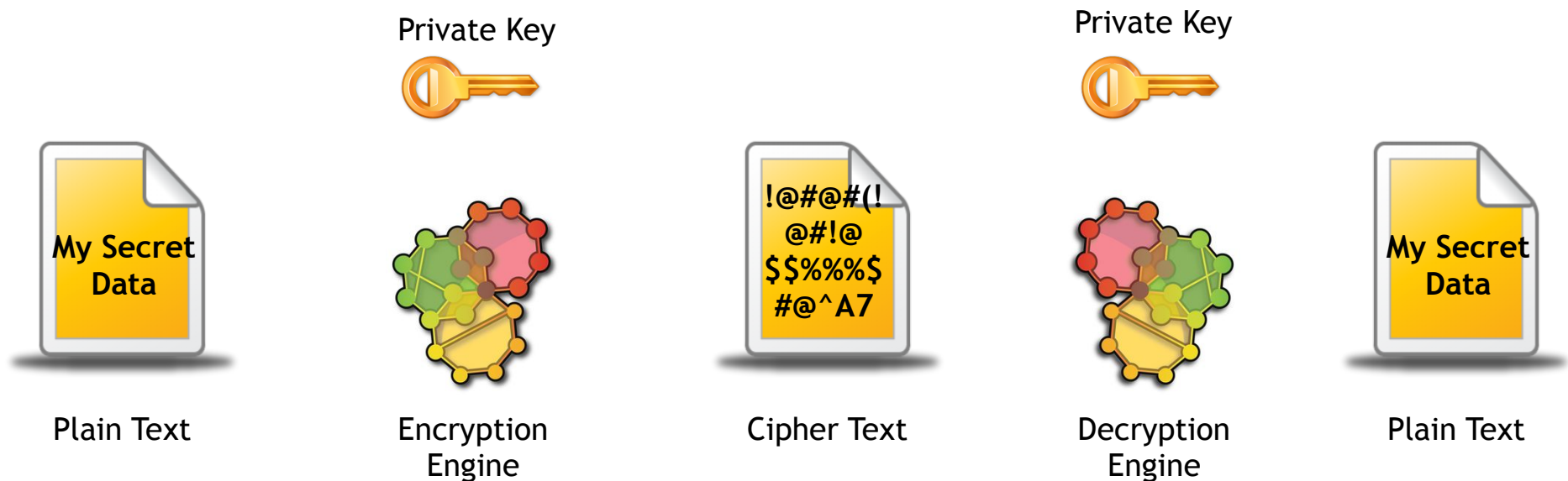
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Authentication: The process of proving one's identity.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent this message.
- Key exchange: The method by which crypto keys are shared between sender and receiver.



Performance and Security

Cryptography - Types

- Secret Key Cryptography (SKC)



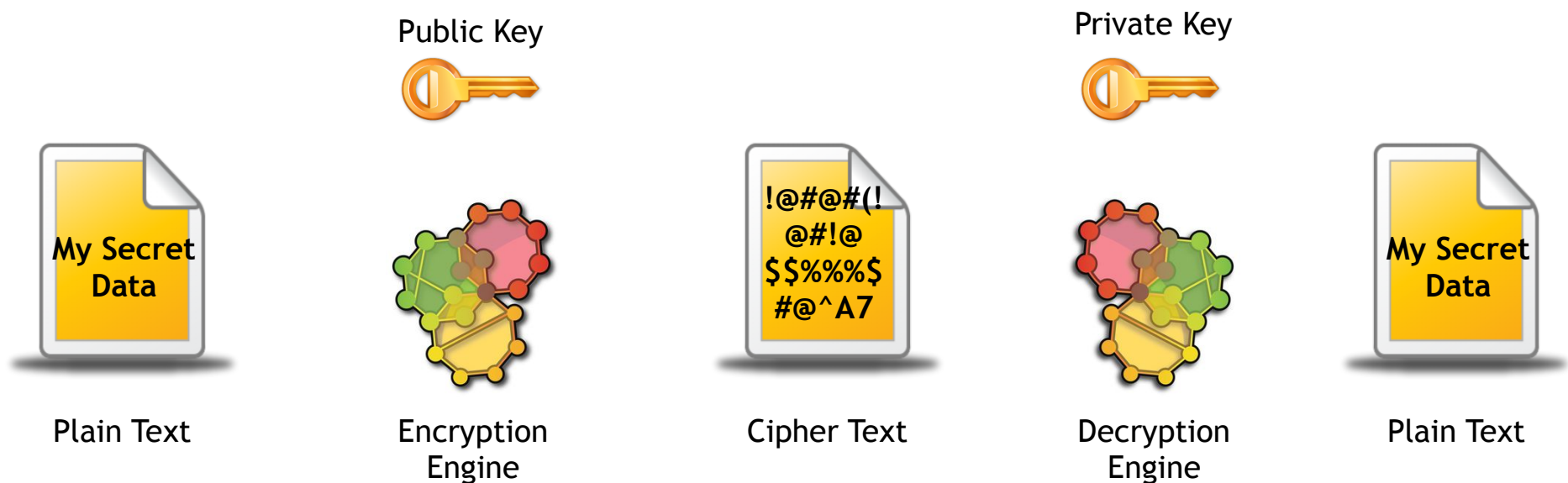
- Symmetric Cryptography, since both Encryption and Decryption use same key



Performance and Security

Cryptography - Types

- Public Key Cryptography (PKC)



- Asymmetric Cryptography, since both Encryption and Decryption use different keys



Performance and Security

Cryptography - Types

- Hash Functions



Plain Text



Encryption
Engine



Cipher Text

- Sometimes called as Message Digests and One Way Encryption



Performance and Security

Privacy



- Devices are interconnected globally making it expose the sensitive information leaking through unauthorized access
- Most of the devices may be transmitting the user's personal information such as name, DOB, address, card detail and much more without encryption



Performance and Security

Privacy Considerations



- Control the sharing of data collected by IoT Devices
 - Determine who has access to the data from devices in your home, car etc.,
 - Ability to Mute and Hide devices
 - Control third party access
- Have clarity on what information is collected and shared, when and with whom.
- Identify the online and offline devices
- Control one's digital footprint, especially from IoT devices in intimate settings and trace the information flow



References



- <https://www.shopify.in/encyclopedia/benchmarking>
- <https://ieeexplore.ieee.org/document/8088251>
- https://www.researchgate.net/publication/328051666_Service_Provisioning_in_Vehicular_Networks_Through_Edge_and_Cloud_An_Empirical_Analysis
- <https://www.garykessler.net/library/crypto.html>



Thank You