Fast Facts

- IoT technology can eliminate 25% of low-speed collision property damage
- Automotive Insurance premiums are expected to drop by $86-$172 billion by 2025
- Ship and train maintenance is expected to create up to $67 billion in global economic impact
- Vehicle maintenance is estimated to drop by 10-40% and up to 5% longer life by 2025.
- Condition based maintenance of aircraft, including military, could have a $44-$103 billion impact

Internet of Things (IoT) for Transportation

The Transportation industry, including trains, planes, ships, and automobiles will benefit from Internet of Things innovations by reducing costs, improving efficiency and customer satisfaction, and even create new business models. Insurance premiums will go down as the automotive industry rolls out IoT-based braking systems and the ability to find stolen cars. Airline carriers will reduce the cost of maintenance, reduce down-time, and lengthen the life of equipment by switching to real-time, predictive maintenance. Like software vendors today, equipment manufactures will gather usage data to improve their future products. Connecting vehicles to the Internet and collecting valuable usage and maintenance data could have almost three-quarters of a trillion-dollar economic impact globally by 2025.

IoT Demands Different Security

The technologies we have used to protect traditional transportation communications for the past 20 years are not the right fit for the Internet of Things revolution. Connected vehicles to the Cloud demand a holistic security solution that is purpose-built for IoT. Traditional security solutions use Internet technology that was designed for anonymous browser to server communications. Browsers exchange (in the clear) the minimum acceptable security protocols necessary to establish a connection. However, IoT innovations today are specially designed and connected for specific intentions. Unknown connections can be rejected and security protocols can be agreed upon ahead of time. This type of IoT solution is fundamentally more secure and easier to control because the devices and the hosts are all known entities with closed methods of communicating. However, new IoT innovations have created other challenges.

IoT Challenges for Transportation

- Authentication of approved host connections to vehicles
- Increased data exposure in the Cloud and across networks
- Wireless data speed and cost
- Ensuring security and real-time usability with Big Data in the Cloud

CENTRI IoTAS - Internet of Things Advanced Security

Unlike security solutions for the broad *Internet*, those designed for *the Internet of Things* can define exactly which devices can connect and how they will secure their data, *before they begin communicating*. By encrypting and compressing the data as it's created, as it's delivered, and even as it's stored on servers, IoTAS provides the simplest yet the most comprehensive and secure solution for IoT projects.

IoTAS was designed to protect resource constrained IIoT devices and their data while in use on the device, in motion across the network or at rest in storage. IoTAS employs a trusted device model without vulnerable certificate exchanges so only known endpoints are connected, eliminating potential vehicle hacks. Usable data is protected from internal rogue operators and external hackers. Man-in-the-middle attacks are exposed and Denial of Service (DDoS) attacks launched from devices can never begin when the device only accepts verified commands protected by IoTAS.

IoTAS

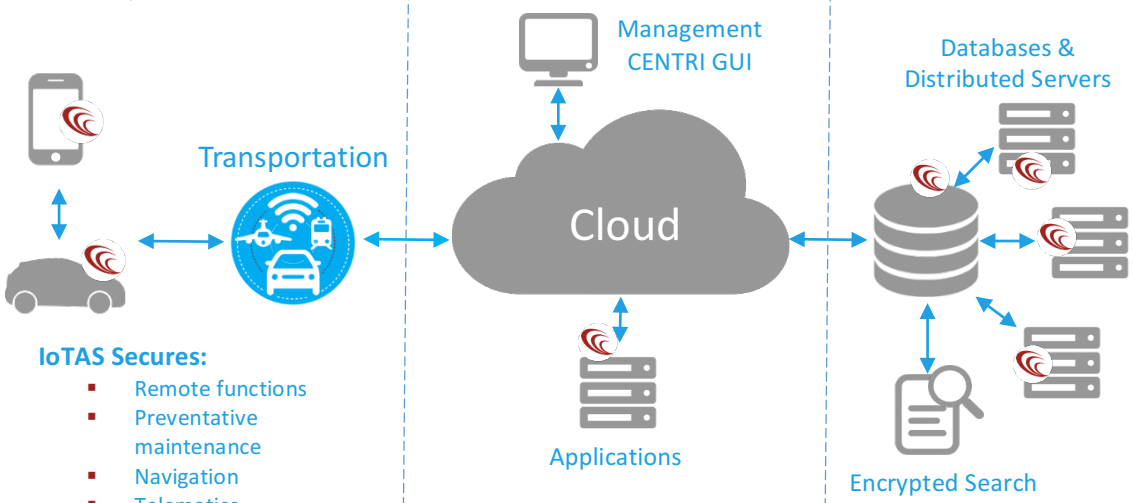
Internet of Things **Advanced Security**

IoT Endpoint & Data Integrity:
- Device Authentication
- Secure Data at Rest
- Secure Data in Motion
- Data Optimization

IoT Cloud Protection:
- Secure Data at Rest
- Data Optimization

IoT Data Visibility:
- Analytics
- Forensics
- User Management
- Encrypted Search

IoTAS Deployment:
- Cars, planes, trains, ships
- Mobile applications for predictive maintenance
- Cloud
- Databases and distributed servers



IoTAS Secures:
- Remote functions
- Preventative maintenance
- Navigation
- Telematics

CENTRI IoTAS vs. Alternatives

Security solutions should be evaluated by the level of security they provide vs the impact to the overall project. The following two axes provide the best practices you should follow when evaluating any IoT security solution.

Axis 1: Security Quality

Cloud: The approach of securing the data before it is transmitted, between trusted devices, eliminates the Cloud/network issues like man-in-the-middle attacks and mitigates DDoS attacks. Unlike traditional SSH, no information is passed in the clear – so no agent can sit in-between and pretend to speak the same language. In addition, DDoS attacks are reduced by a factor of 4 since the usual anonymous introduction between devices is eliminated. When the device and the data are secured with IoTAS, any potential network breach is made irrelevant.

Data: Bad actors can come from inside or outside an organization and your solution needs to take data security into account on the device, in transit, and once it gets to the servers in the Cloud. IoTAS uses advanced encryption to protect all data in transit between any endpoints and at rest. A disgruntled employee can take proprietary process information or hackers can use social engineering to login and download customer data, but it's unusable on any device that is not authorized. Applications on trusted devices (smartphones, servers, work stations) transparently access the information; any data downloaded to thumb drives or unauthorized devices cannot be decrypted and is worthless.

Device: The security of vehicles is critical not just for protecting consumer data but ensuring the safety of operators and passengers. The more that we automate the more vulnerable we become to hackers without the right security solution. IoTAS provides device integrity so that any connection from an untrusted source is immediately dropped. Malware delivered from untrusted connections is eliminated and only your trusted commands are allowed.

Peer to Peer: Unlike most IoT security solutions, IoTAS does not require an Internet server to secure the communication. For example, a vehicle can connect to a trusted device all without ever connecting to the Internet.

Axis 2: IoT Solution Impact

Solution Footprint: CENTRI has the smallest device footprint to accommodate a wide range of transportation equipment. Depending on the device and network requirements the CENTRI solution can be as little as 50kB.

Power Efficiency: A small form-factor device is always limited by the power it consumes. A battery-operated handheld device may require large amounts of processing power which can run devices hot and limit battery life. IoTAS uses cache mapping technology and efficient algorithms for 20% less CPU utilization and up to 30% more uptime of IoT equipment.

Bandwidth and Cloud Storage: Reducing bandwidth is important with cellular or satellite connected devices where IoT data transmission can be costly. IoTAS compresses the data up to 80% depending on the type of data, (e.g., text, audio, video) thereby speeding delivery and reducing the overall costs of adding bandwidth or Cloud storage.

Delivery Speed: Many IoT environments feature thousands of devices sending large data sets. IoTAS is 100-150x more efficient establishing a handshake (i.e., device identification) required for communication than the standard SSH protocol (2-3 milliseconds vs 250-300 milliseconds).

Cost: IoTAS offers less Total Cost of Ownership (TCO) for several reasons including 4-8x server efficiency, "vault-less" key management technology, and a developer-centric complete solution launching in days vs. months for DIY solutions.

Summary

CENTRI IoTAS – Internet of Things Advanced Security, offers transportation companies looking to secure their vehicles, sensors, gateways, data, and Cloud, a complete solution that meets the unique requirements of real-time connections with thousands or millions of endpoints. IoTAS also solves the security challenge for consumers and companies as it protects IoT data in the Cloud in multi-tenant and shared environments. The solution uses cache mapping technology and efficient algorithms for lower CPU utilization, heat reduction and increased uptime of devices. When you make the security decision for your IoT project make certain your solution takes into account your needs today and into the future. Unlike DIY or repackaged enterprise solutions, CENTRI IoTAS delivers a security platform that is purpose-built for the trusted, known endpoints of the transportation industry.

*Estimates and forecasts are taken from the McKinsey Global Institute "The Internet of Things: Mapping the Value Beyond the Hype", June 2015. IDC press release, "Apple Debuts at the Number Two Spot as the Worldwide Wearables Market Grows 223.2% in 2Q15", August 27, 2015. Gartner press release "Gartner Identifies the Top 10 Internet of Things Technologies for 2017 and 2018", February 23, 2016. ISACA's "THE HIDDEN INTERNET OF THINGS ISACA 2015 IT RISK / REWARD BAROMETER", 2015.

About CENTRI

CENTRI provides a complete, advanced security solution for the Internet of Things. Our flexible, software-only platform enables thing makers and developers to quickly get to market with purpose-built IoT security to protect their data from chip to Cloud. CENTRI eliminates the risk of data theft and delivers device integrity with modern, standards-based technologies for the connected world. **For more information visit** centritechnology.com **or email us at** sales@centritechnology.com.