PIPELINE | VOLUME 18 | ISSUE 9

PL

TRANSFORMING GOVERNMENT USING BLOCKCHAIN

WITH: TNS Total Network Services

IOT DEVICE SECURITY

THE BACKBONE OF MASSIVE IOT

FEATURING: & everynet

MAKING IOT SMART

THE NEW SPACE RACE

ROBOT AS A SERVICE FOR SMART AG

THREATS TO ENTERPRISE IOT

FUELING IOT MOMENTUM

PROTECTING A PRECIOUS RESOURCE

PRIVATE APN FOR IOT

CEO THOMAS CARTER & SVP KEVIN L. JACKSON, TNS

THE DEVICE REVOLUTION

Pipeline

Volume 18, Issue 9

Federal Government Transformation Using Blockchain

By Scott St. John

There are nearly eight billion people on the planet, but **connected devices outnumber us humans two to one**. Adoption shows no signs of slowing, as the proliferation of the Internet of Things (IoT) continues to accelerate. The IoT is creating many new benefits, opportunities, and use cases spanning smart agriculture, appliances, cars, cities, and devices. IoT device manufacturers, solution providers, and telecom service providers are all racing to capture their share of this enormous opportunity.

However, these new opportunities also bring a level of risk with them, to both the device and data, that must be taken into consideration. The size, scale, and sophistication of the most recent IoT cybersecurity attacks serve as a warning, with quantum-resistant cybersecurity threats materializing in the not-too-distant future.

Government agencies, universities, nonprofits, and the private sector are turning to emerging technologies to help them transform, efficiently capitalize upon the IoT opportunity, and to address the risks. This includes the adoption of technologies such as Artificial Intelligence (AI) and Robotics Process Automation (RPA). Beyond these, new and emerging technologies are flourishing—with significant transformative potential for IoT device security. This includes technologies like the **Universal Communications Identifier (UCID)**, a unique identifier for a device on a network; the blockchain, a distributed ledger shared with the nodes of a computer network to guarantee security; and Non-Fungible Tokens, cryptographic assets on a blockchain that cannot be replicated. The combined practical application of these technologies—implementing UCID on the device, using NFTs, and putting them on the blockchain—ensures that the device itself is authenticated on a network that cannot be corrupted. This is a giant leap forward—and it's happening now, in the United States government.

Introducing EMMA

The US Census Bureau, United States Department of Commerce is undertaking a massive digital transformation in preparation for the 2030 Census. The Bureau is setting its sights on updating key functions such as claims processing, operations synchronization, and data governance. As part of its transformation, the bureau is implementing the newly developed **Electronic Medical Mobile Application (EMMA)** to modernize how workers' compensation, property and tort claims are filed when an injury or incident occurs. EMMA will be the first blockchain implementation at the Census Bureau and—with 500,000 anticipated field enumerator users—it's the largest blockchain project currently underway within the federal government.

EMMA is the product of a collaboration between Forward Edge-AI, Rypplzz, and Total Network Services (TNS). Pipeline recently had the opportunity to discuss EMMA with CEO Eric Adolphe of Forward Edge-AI, CEO **Thomas Carter** of TNS, and its SVP of Channel Sales

Kevin L. Jackson. The conversation explored EMMA and the use of these advanced technologies in the federal government for the US Census. It also examined how the EMMA project can be applied to other innovative government, enterprise, and telecom use cases and how this unique combination of technologies can be leveraged to efficiently and securely seize the IoT opportunity.

Protecting data, devices, and workers with blockchain innovation

Every ten years, the US Census Bureau tackles the mammoth job of counting all the people in the country and recording basic data like age, sex, and race. Census data is critically important to the everyday lives of citizens, as it informs government and policy decisions from infrastructure to determining the number of representatives in Congress. But gathering Census data is anything but straightforward. The recently completed 2020 Census relied on 52 legacy systems. The Census Bureau is now focused on leveraging sophisticated, new technologies—including AI, blockchain, chatbots, NFTs, RPA, and UCID—to synchronize operations, eliminate legacy systems, protect data, and significantly improve device security during the 2030Census. To collect data, the Census Bureau deploys 500,000 field employees with mobile-connected devices to canvass, document, and report results nationwide. It can be dangerous work, exposing workers to animal attacks, injuries, or property damage claims. There are thousands of workers' compensation, property damage and tort claims filed during each Census. Historically, filing a claim has been a labor-intensive, manual, and bureaucratic process. The paperwork alone can take 72 hours to complete, and then information must be shared within the Bureau's three internal offices and is subject

to compliance with medical data disclosure and Title 13 restrictions. Simply the wrong person opening the wrong drawer of a file cabinet can be a data breach and subject to claims.

EMMA has been designed to modernize the Census process through the practical application of emerging technologies. During the 2030 Census, EMMA will be used to protect devices, data, and workers. EMMA will provide Census workers with a single, intelligent interface as a mobile device application that understands natural language, can notify the proper authorities, process images to assess damage, automatically complete reports, and distribute the required documentation to the necessary departments within the Bureau. All within minutes, providing a monumental improvement to the customer experience (CX).

It will also unlock efficiency through the elimination of five legacy systems and other manual processes. Using RPA, EMMA will perform once-manual tasks, parse trigger-free error responses, and reduce the time to complete claims forms. "EMMA will reduce the manual process of filing a claim from 72 hours to two minutes," Forward Edge-AI's Eric Adolphe said. Data also will enable greater visibility into why and where injuries happen, enabling more informed decisions about safety precautions and shaping communications to better prepare field enumerators. Through the use of blockchain, NFTs and UCID, EMMA will also provide unprecedented mobile-device security. Eric underscored the future potential: "As the first application of blockchain in the Census Bureau, this project is pioneering the way for other government and enterprise applications in the future."

As Eric and his collaborators from TNS note, EMMA is a model for business-to-government (B2G) commercialization and market development—and represents an entry point to a huge potential market for these emerging technologies. It also demonstrates the real-world potential for these technologies, such as blockchain, and accelerates their adoption. To put this into perspective, the cryptocurrency market has been valued at its recent height at **$3 trillion**, while US government healthcare is projected to have a national expenditure of **$6.8 trillion by 2028**. And that's just one B2G use case.

EMMA's use of emerging technologies including blockchain, NFTs, and UCID also illustrates a quantum leap forward for data and device security which is integral to the success of the IoT.

Supporting innovation through transformation

On the surface, the United States government might seem an unlikely innovation driver, but it has a 40-year history of leveraging private industry for innovation through the National Science Foundation's

There's an entire market built around the selling of medical data and it's up to 50 times more valuable than credit card information.

Small Business Innovation Research (SBIR) program. The SBIR was established in 1982 to fund innovation in small business, with the idea that the federal government could accelerate ground-breaking work and spur economic growth. The SBIR program has since become the premier seed capital program in the world, giving companies like 23 and Me, Google, iRobot, Lasik, Qualcomm, Genentech, and others the backing to accelerate the development of transformative technology products, services, and business models. Through phased funding, SBIR grants invest in, de-risk, and commercialize products for B2B, B2C, and B2G markets. EMMA is the Census Acquisition Team's first Phase III SBIR and the first-ever use of the sole source authorities of the SBIR program by the Census Bureau.

Seizing opportunities and mitigating risks

Combining AI, chatbots, and RPA is a significant step forward for CX, digital transformation and optimizing operational efficiency. But EMMA's use of emerging technologies including blockchain, NFTs, and UCID also illustrates a quantum leap forward for data and device security which is integral to the success of the IoT.

Kevin L. Jackson of TNS told *Pipeline*, "Change is happening fast. Our virtual lives are as important as our physical lives." CEO Thomas Carter added, "Our devices are an integral part of everyday life, and we need to protect them and the data they collect, store, and transmit. It's about protecting your physical and virtual existence, and your digital legacy."

TNS leverages blockchain to provide real-time software and hardware verification via its patent pending UCID technology. Together, Forward Edge-AI and TNS are enabling device verification via EMMA for the Census Bureau to prevent device duplication and the use of counterfeit devices. They are also creating an immutable trail of custody on data for all medical claims related to field injuries and incidents.

"Via device orchestration and security, we can make sure that information on Census workers is not inadvertently shared, triggering HIPAA violations and more," Eric said. Beyond EMMA and the census, the potential for this technology is enormous, with a total addressable market of billions of connected devices that **Transforma** has predicted will grow to $1.5 trillion in value by 2030.

As the IoT momentum accelerates and the world becomes more dependent upon connected devices, end users may simply assume that their devices, data, and the underlying networks are secure. But this may be a gross miscalculation.

In 2008, **Kevin Fu** from the University of Massachusetts, Amherst demonstrated the real cybersecurity risks for surgically implanted connected medical devices including cardiac pacemakers and defibrillators. Fu was able to hack these implanted medical devices to drain the battery that was meant to last years to just weeks; and use them to shock a heart with 700 volts of electricity. Since then, there has been an **increase in the number, sophistication, and variety of attacks** on connected medical devices, **including insulin pumps**. And that's just the device risk. There's an entire market built around the selling of medical data and it's up to **50 times more valuable** than credit card information. Quantum-level cybersecurity attacks will be increasingly focused on the advanced persistent threat or sabotage levels, in addition to data theft and ransomware.

Medical identity data can include social security numbers, credit card numbers, and much more. Hacking sensitive medical information enables someone to make an insurance claim on your behalf, or to collect on an insurance policy. But it's not just about the value of medical data to hackers. A growing market will use medical data and history for diagnoses, tailored care, insurance decisions, and more. The consequences for medical score data can and will be far-reaching.

The recent decision by the US Supreme Court to **overturn Roe v. Wade** combined with the Affordable Care Act (ACA) amplifies this concern. Setting the headlines aside, Roe set a limitation of the government's authority to make decisions over one's own body. The historic decision to overturn Roe now creates the potential to give this authority to the same institution making and paying for medical decisions under the ACA, affecting millions of Americans. The implications for the sharing, use and transmission of medical data are still unknown. But, one can imagine the risks the unintended use or misuse of this information may create.

The rapidly shifting landscape, evolving opportunities, and accelerating adoption of connected devices across industries introduces new complexity for device and data security. This is especially true with the development of large-scale quantum computers that create greater risk in the wrong hands. But Forward Edge-AI has as solution for that.

Under a Cooperative Research and Development Agreement (CRADA), Forward Edge-AI and the National Security Agency (NSA) are commercializing a quantum-resistant encryption device, called Isidore Quantum, to augment IoT and other edge devices. Isidore offers low-cost (under $500), quantum-resistant encryption to protect a wide range of public and private infrastructure systems, including IoT, SCADA, the growing Internet of Medical Things (IoMT), autonomous vehicles, VIP mobile phones, and much more. Given the value of and risk to medical score data, the IoMT use case is a priority, and potential government implementation to protect medical devices is on the horizon.

The combination and application of technologies including AI, blockchain, NTFs, RPA and UCID offers enormous potential—in government and well beyond. "With so many use cases, government is ripe for the adoption of these emerging technologies," Eric said. "As we demonstrate the successful application of advanced technology for half of a million users and devices within the federal government, the potential to expand is virtually limitless."

The success of EMMA and the tangible application of emerging technologies unlocks the potential for the IoT, transformation, and innovation across nearly every industry. The massive number of connected devices coming online is staggering, and automation is the key to harnessing efficiency at scale. Many have tried to seize this opportunity ignoring the importance of security and have paid the price. Their names are now synonymous with breach. Think Colonial Pipeline, Dyn, and Solarwinds. TNS, Rypplzz, and Forward Edge-AI have created a unique solution that combines both efficiency and security and it's getting noticed, attracting millions of dollars in investment to make this unique technology offering a reality.

EMMA serves as an important proof point for the solution as well as the underlying technology, which are key to unlocking efficiency, while mitigating the risks, to capitalize on the IoT opportunity. It's also essential to ensuring the safety and security of our evolving, global, and increasingly connected society. Innovation may not be occurring where you would expect, but it is happening where it is needed, and it's needed now.

2173 Salk Ave. Suite 250
Carlsbad, CA 92008

+1 (760) 260-8144
hello@tnscorp.io
www.totalnetworkservices.io

About TNS

TNS is a blockchain transformation company seamlessly transitioning the connected world into the blockchain economy. Our mission is to make the transition into this new digital world simple, standardized, and secure. With solutions spanning across crypto payments, IoT device management, global network hosting, and even NFT adoption, TNS leverages the full breadth of the blockchain to help enterprises and individuals solve some of the most pressing challenges in our world today. Now you can become part of the blockchain revolution. Visit **www.totalnetworkservices.io** to learn more.