Deloitte.

The Deloitte On Cloud Podcast

David Linthicum, Managing Director, Chief Cloud Strategy Officer, Deloitte Consulting LLP

Title: **Leveraging cloud and other innovative tech to combat smartphone fraud**

Description: Smartphones are the center of our world, but, unfortunately, they are also the latest vector of attack for many criminals—and the number and severity of attacks is growing. So, smartphone security has become a hot issue across the globe. In this episode, David Linthicum talks with Kevin L. Jackson about how innovative companies—some at the behest of government agencies—are leveraging cloud, blockchain, AI/ML, and crowd-sourcing to combat smartphone hacking, phishing, and counterfeiting.

Duration: **00:23:55**

David Linthicum:
Welcome back to the On Cloud podcast. Today on the show I'm joined by Kevin L. Jackson, who was a guest of the show back in 2019. Kevin, it's great to have you back on the show today.

Kevin L. Jackson:
Yeah, thank you for having me back. It's an honor.

David Linthicum:
Well, it's our honor. It's our honor. It's all our pleasure. And look at what you accomplished. I always forget. I mean, we've known each other for years, but you have 300,000 followers on social media, he's the host of the Digital Transformer podcast, provides consulting and digital media services to leading technology companies. His client list includes Microsoft, AT&T, AT&T Business, and IBM. He also serves as adjunct professor at Tulane University. Executive experience includes Vice President at JPMorgan Chase, IMB Worldwide sales executive, and SAIC director of cloud solutions. His education includes MS computer engineering, MA strategic studies, and BS in aerospace engineering. Also, you went to the Naval Academy. Is that right, Kevin?

Kevin L. Jackson:
Yeah, go Navy, beat Army. That was a great game last weekend.

David Linthicum:
Figured we'd get to that one during the podcast. Kevin is also a *USA Today* and *Wall Street Journal* bestselling author. His books include *Click to Transform* in 2020, and *Architecting Cloud Computing Solutions* in 2018. All right, well, catch us up what you've been doing for the last couple of years, Kevin. Doesn't look like you've got much time to do anything with all that stuff going on, so what have you been focusing on?

Kevin L. Jackson:
Well, to be honest, I've been really focused on leveraging cloud for some of the other business technologies that are layered on top of cloud computing. Things like blockchain and robotic process engineering, and these are—and machine learning, artificial intelligence. All of these things now are becoming sort of table stakes in business models, and they wouldn't any of them—none of them would be possible without the underlying cloud computing foundation.

David Linthicum:
Yeah, it's amazing to me the versatility of these smartphones we hold in our hands. I know everybody looks at them. They just kind of morphed over time into a very simple communication device just doing text and e-mail and voice, initially just doing voice with a traditional feature phone. And now they really are these supercomputers that we hold in our hands, and the reality is that lots of information flows through there that needs to be protected. And this is something that's just kind of emerging today and people are considering how to do this best. And so, you just described some of the mechanisms we're dealing with—blockchain technology, machine learning, the ability to deal with high-end encryption services, ICT, supply chain stuff. So, catch us up. What's state of the art in that world and what should we be looking for in terms of emerging technology around the smartphone security space leveraging cloud computing?

Kevin L. Jackson:
Well, you remember a long, long time ago, I mean, I'm belying my age, where your workplace had the best technology. You would have to go in to work to use e-mail because you didn't have anything at home. And then it sort of shifted with the consumerization of information technologies and computers, when now the best IET was at home with the entertainment industry. And now it's really your personal communications network. You don't use—you were talking about the smartphone, but yeah, you may use your smartphone for work or business, but you use it more to keep in contact with your family, to track your kids, to get information on your friends or your business partners. So, the smartphone has really become the center of our world, I was on a show recently where the host said, "The only thing I want when I walk out of the door are my car keys and my smartphone."

They don't even carry a purse or wallet anymore. So, what's happening right now is your world is your smartphone. And that represents your personal communications network, and today it's under vicious attack because that's where the money is. In fact, the Communications Fraud Control Association did a survey and showed that fraud over telecommunications networks was about $28.3 billion in 2019. And these fraud types include—it's Christmas—online shopping, internet services, prizes. Sweepstakes and lotteries and telephone and mobile services. So, now, since that's where the money is, the fraudsters and cybercriminals are attacking your personal telecommunication network, attacking your smartphone.

David Linthicum:
And so, this is about the ability to leverage cloud computing for security capabilities, and that's kind of a bit of an odd reach for people who understand the phone. Now, there's—I'm holding onto a phone. It is a device that I can see. Now, it maybe communicating to backend services via the cloud, but I don't necessarily view this as something that can be protected by the cloud. That's wrong, and how is that technology moving these days?

Kevin L. Jackson:
So, actually, I mean, we know what supply chain is now based upon our experience of COVID. You go into the store, and the shelves are empty. But there's also an information technology supply chain, and one terminus of that is your smartphone. That's how you receive information. But 6.5 percent of all products, devices on the network have counterfeit parts, and nearly 20 percent of all mobile phones that have been shipped are actually fake. That's one reason why the Telecommunications Industry Association actually initiated a supply chain security standard initiative this year, 2020, to improve the supply chain security and to incorporate new requirements to address this modern network. Because every device has an identifier.

Some have a mobile equipment identifier. Others have—that's an MEID. Others have what's called an IMEI, or international mobile equipment identity identifier. So, this enables your service provider to actually track that device, but you can also use it to protect that device. And this is what I've been actually working on in the past year. It's called an enhanced mobile equipment identifier, or EMEID. And we're talking those identifiers and putting them on a blockchain or distributed ledger technology that sit on top of the cloud. This actually tokenizes these equipment identifiers. I'm sure you've heard of the NFT art craze.

David Linthicum:
Yep.

Kevin L. Jackson:
Well, that's really—the NFT stands for a non-fungible token, and that's tokenizing art. Where we're taking that approach and tokenizing your smartphone and applying it to cybersecurity because since we can keep the identity unique of your smartphone, we can now track or verify, for instance, that the

software that you have on your software on your smartphone hasn't been changed. We can verify that you have a real smartphone and it's not a counterfeit smartphone that could be spied upon. And the other aspect of that is when people are trying to phish, i.e., fraudsters are posing as your friend or as a government agency, we can actually flag that that communication is fraudulent.

David Linthicum:
So, my smartphone could be betraying me. In other words, I may have gotten a smartphone that's been manufactured with not only counterfeit parts, but parts that may be have embedded firmware where it's able to act upon the information and pipe some of the information out of the phone. Kind of making me mad. I paid $1,100 for this thing. And the thing is the cloud has the ability to kind of find these things. Is it more of an alerting capability? Is it the ability to find and destroy? Is it the ability to just, in essence, layer security into something that—I guess this thing's going to be entrusted, right. So, therefore, if you're going to have a true trust-nobody security system, the phone is something you don't trust as well.

Kevin L. Jackson:
Well, yeah, you can't. But everyone's heard of crowd sourcing. What if you crowd source the cyber environment of all of these smartphones, and you can use—you call it swarm intelligence, but it's really artificial intelligence and machine learning to collect the connection of all these smartphones, and it can help you point to the nexus of the fraud attacks. And all that is being done on the cloud. So, tests have shown that if a fraud attack happened three times, you can actually identify it as fraud, and then everyone that's in that network can now be alerted if they are attacked. So, it's crowd sourcing cybersecurity.

David Linthicum:
That's cool. And you think about it, we're getting—still leveraging the blockchain model and the ability to do things with peer-to-peer validation, which if you think about it, it's pretty brilliant compared to the centralized security models that we've had in the past and centralized funding networks and things like that. So, how would blockchain be leveraged in terms of mobile security, and where would the mechanism exist? Would it exist in the—would it exist in the cloud, or exist on the phone, or between both?

Kevin L. Jackson:
So, actually, it exists in the cloud. The block—each of the devices have a unique identifier like I talked about before, and the information, the cybersecurity information is attached in the meta data to that unique identifier on the blockchain. So, that enables the machine learning to actually compare networks and attack in real time. Now, I don't need to know the details—your personal details to do this, right. All I really need to know is like the—that the software, for instance, on your device is the same software that was installed on a device.

Any changes may indicate an attack. And I can also—another piece of technology is the ESIM that's coming to market. And everyone in their smartphone, you have a physical SIM card, and that's really being replaced by an electronic SIM card, a programmable SIM card. And this will help you with instant network connectivity, customizing the services that come to your device, remote provisioning of new services, and global roaming between different network or telephone service providers. So, if you can do this security crowd sourcing across different telcos, you now have a powerful cloud-based backend to protect the user.

David Linthicum:
That's very cool. So, let's talk about 2022 next year, some of the security advancements that we're going to start seeing. Some of the things you list in your article I think I'd love to hear more about, Gabriel® Crypto and Forward Edge AI, ComSovereign. Tell me about those few things.

Kevin L. Jackson:
So, Forward Edge AI is really a unique company. I don't know if you or your audience have heard about a US government project called the Small Business Innovative Research, or SBIR. Well, in that government program, they actually look for small businesses with innovative ideas, and they give them seed money. It's like investment to investigate how to make these ideas into real products. Much of that money is funneled through the National Science Foundation, and Forward Edge is basically an SBIR company.

And they are using these advanced technologies to verify personal contact devices, detect counterfeit smartphones by using these advanced things on top of 5G networks which are being deployed rapidly, and they're using natural language processing. So, their product is Gabriel® Crypto, And so, you can actually download this to your own smartphone and participate in this crowd-sourced cybersecurity defense.

Ripple is another company that's leveraging geospatial technology to actually help characterize the cybersecurity environment around you. So, it's great to know the types of attacks that are occurring, but you really want to know where they are occurring, also where they're originating from, and pass that information to law enforcement so that we can stop these attacks. So, by understanding one terminus—your device—with the EMBIED and applying this geospatial technology once again in the cloud, you can actually stop these attacks. And the other company,

ComSovereign, they actually support first responders with advanced wireless technology and private wireless 5G network so that the police and the ambulance and for medical care and even for disaster response, FEMA, can bring their own wireless network into an area that has been devastated, and all the first responders can communicate, but you also need that network to be protected because the bad guys don't care if it's a first responder. So, they're using the ESIM technology embedded into these product networks with the EMEIED and a Ripple geospatial technology to really program protection into these first responder networks. And that's coming in 2022. They actually put their system in a drone, so that the drone would sort of fly above the area and provide protected high-security wireless data connectivity.

David Linthicum:
That's amazing just the amount of security technology that has to be created by just the simple use of a phone. But like I was saying, we're moving these devices as primary—the primary way we're going to consume data, consume information, consume cloud and a lot of personal stuff, how we're doing businesses, things like that. and it just seems like the ability to crack and hijack these things is getting pretty scary. So, where are we going to be looking to next year in terms of technology updates, and how would people kind of align their businesses to start moving in these directions, not necessarily leveraging this technology now. Sounds like some of it's still being baked, but the ability to kind of plan for it. What should they be doing in terms of how they deal with cloud security now, how they train their people, how they prepare for this kind of next generation mobile security stuff?

Kevin L. Jackson:
Well, one of the biggest challenges across business is really understanding the data, properly categorizing the data, and understanding who's using your data. So, by connecting verifiable—having a verifiable record of devices and data, you can have really a verifiable automated record of network security operations. Now, and this reduces the actual labor that you need and increases the visibility across your network. So, one of the biggest challenges is companies will use SIM, or security incident event management software, to determine if there's been a hack.

But the biggest problem is not having enough people to look at the alerts. Now, you can actually take the alerts associated with devices, put that information on the blockchain, and automate this alert. It also can provide insight into your software across your network. So, if you can take your device and use something like the enhanced MEIED to monitor and provide alerts in real time if that software is changed, you can actually get ahead of the issue. And the use will rush to use open source.

So, by leveraging digital signatures of open-source software, you can be assured that you're using software that has not been tampered with by an attacker. This also helps you with your change management process documentation within your organization to make sure that you stay on top of any vulnerabilities that may be put—may be discovered by NIST and the national vulnerability database. It also really enhances mobile device traceability and be able to track any hardware or software component changes. So, this not only helps the enterprise in protecting their environment, but it reduces the cost that they have to pay to protect it and things like cybersecurity insurance. The cost of that can be reduced by having these technologies and these capabilities in place. So, 2022 will give these organizations many more advanced methods of increasing their margin and reducing their cost and enhancing the protection of their data.

David Linthicum:
Yeah, I'm looking forward to this kind of emerging of this technology because the security has to be there in order for us to leverage these devices. You can't have one without the other, and so if this is the way the world is going, moving to cloud, moving to mobile devices, edge computing, IOT, and all these sorts of things, we have to think of new and innovative ways to secure them. And I enjoyed the deep dive because it was learning myself where this world is. I mean, I follow cloud computing pretty closely but not necessarily mobile security as much. So, where can we find you on the web, and where can we point to your books and other ways we can learn about Kevin?

Kevin L. Jackson:
Thank you. I'm on many channels. Twitter, I'm @kevin_jackson or Kevin L. Jackson on LinkedIn. And my podcast, Digital Transformers, you can find that on and subscribe, please, on Amazon, on Apple, or Google Podcasts, as well as Stitcher. So, please reach out and be glad to talk with you.

David Linthicum:
Yeah, and just some personal notes about Kevin, you know, back in the day when cloud started, there was only a few people around who kind of got it, and he was one of them. And so, we've been friends for a long time, and I follow him directly, and he is one of the pioneers in cloud computing, and someone who's actually looking to take technology to the next level as we saw in this conversation. So, if you enjoyed this podcast, make sure to like us and rate us and subscribe. You can check us out—you can check out our past episodes, including those hosted by my good friend, Mike Kavis. Find out more at deloittecloudpodcast.com. if you'd like to contact me directly, you can e-mail me at dlinthicum@deloitte.com. So, until next time, best of luck in your cloud journey. You guys stay safe. Have a good one. Have a happy new year.

David Linthicum
If you enjoyed this podcast, make sure to like us, rate us, and subscribe. You can also check out our past episodes, including those hosted by my good friend, Mike Kavis. Find out more at "deloitte cloud podcast .com" all one word. If you'd like to contact me directly, email me at dlinthicum@deloitte.com. Until next time, best of luck with your cloud journey, and stay safe!

Operator:
This podcast is produced by Deloitte. The views and opinions expressed by podcast speakers and guests are solely their own and do not reflect the opinions of Deloitte. This podcast provides general information only and is not intended to constitute advice or services of any kind. For additional information about Deloitte, go to Deloitte.com/about.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Visit the On Cloud library
www.deloitte.com/us/cloud-podcast

About Deloitte

As used in this podcast, “Deloitte” means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.
Please see www.deloitte.com/about to learn more about our global network of member firms. Copyright © 2021 Deloitte Development LLC. All rights reserved.