Blockchain Cybersecurity for Edge Computing Nodes Such as Digital Twin, and Other Deployed Edge Systems

Michael Wikan
Booz Allen Hamilton
Austin, Texas
wikan_michael@bah.com

Yugandhar Cindepalle
Booz Allen Hamilton
Washington, DC
cindepalle_yugandhar@bah.com

This paper explores the utilization of blockchain-based technologies, applying Physical Unclonable Functions (PUF) to harden complex computing arrays against cyber intrusions, as are present in digital twin installations.

PROBLEM STATEMENT

The accelerated development of new cyber warfare techniques is driving a pressing need for more durable and immutable methods of securing potential access points on cluster computing (edge node) systems currently deployed or those that will be deployed soon. With the advent of quantum computing both by U.S. and peer adversary nations, the need for secure edge systems becomes even more important for law enforcement and first responders, as well as other services like the military and federal law enforcement entities.

These agencies must swiftly modernize their approach to cyber defense by dramatically hardening these vulnerabilities using rapidly deployable, low-cost cyber solutions like blockchain and PUFs at a reasonable cost. These systems must be deployable on current-generation (legacy) systems but also future-deployable on next-generation edge systems as they come online.

The reason for this rapidly accelerating need for hardened and inexpensive cyber defense is the rapid proliferation of cluster computing arrays and sequentially developed technologies like digital twin computing clusters, which take edge nodes and tie them together to create a real-time, addressable, and analytic pipeline that mirrors real-world locations such as airports, ports, military bases, power plants, and even whole cities. These edge node digital twin systems are being deployed at areas of critical security and infrastructure needs, and as such are also the primary access points where bad actors concentrate to breach our cybersecurity to gain information for state espionage, corporate espionage, theft, terrorism, or disruption of these systems for political or terroristic gain.

One can imagine breaching a digital twin of a major U.S. port and modifying the data to disrupt the onloading and offloading of shipping (i.e., changing the shipping schedules). This simple change could disrupt the supply chain across the entire U.S., causing global ripple effects that cost the global economy hundreds of billions of dollars and create subsidiary disruptions in the global labor market. By simply changing a few pieces of data on one cluster compute node, this could contaminate the whole downstream analytics and planning system.

To take advantage of the massive productivity and logistical management gains being realized by digital twin and other Internet of Things (IoT) systems, we must also be cognizant of the intrinsic vulnerabilities such systems create. Blockchain offers a low-cost/high-impermeability solution for deployment on these systems as they come online.

PROPOSED SOLUTION OVERVIEW

We propose the development and deployment of protected cluster networks through the deployment of blockchain-secured access codes and blockchain-secured PUFs to cluster computer networks, as exemplified by digital twin systems.

These digital twin systems are designed to enable real-time design and management of complex, real-world facilities that streamline the information flow of everything including water, power, traffic, security, planning, networks, and any other element contained in the information network. Digital twin systems are being deployed worldwide, not only commercially in the U.S., but also on U.S. Department of Defense (DOD) installations. These digital twin systems offer dramatic cost savings by collating all pertinent data about the modeled area, but this also creates a significant security threat by bad actors who want to steal or alter the data and create secondary downstream security issues with that access.

The digital twin system relies on cluster nodes for reporting, which are either static nodes at specific locations or mobile nodes like augmented reality (AR) headsets such as the Microsoft HoloLens 2 or the Army's IVAS (Integrated Visual Augmentation System) program. This density of smart node devices creates a large computing surface area that can be vulnerable to cyberattack.

This vulnerability is exemplified by the Red Hat cyber testing of the Navy's Littoral Combat Ship (LCS), where during testing, the Red Hat team was able to enter LCS' supposedly secure distributed Smart Node network through a battery system's Wi-Fi and then burrow sideways and seize control of the vessel entirely, driving it in figure 8 patterns around the Great Lakes (Capaccio, 2013).

Blockchain technology offers the means to airlock input/output to these nodes with an immutable verifiable authentication regime. Each node is secured by its own internal firewall that inhibits access to the system, and each other node it communicates with must independently verify access codes that are immutably verified by blockchain-secure protocols.

The addition of PUFs allows an additional hardware security layer to the edge node/blockchain security block by using the PUF fingerprint of the edge node hardware in blockchain to verify the integrity of the hardware as well as the access codes stored in the blockchain airlock. These two systems can report in tandem to create a dual-factor immutable verification code.

This dual-verification system (hardware/software) means that every smart node in a digital twin is independently hardened and verifiable with an immutable record that cannot be broken. This creates layers of hardening at every point of access, degrading the ability of a hacker to get behind a firewall and have free access to a networked computer system. The incorrect interrogation or broadcast of any component (PUF record or blockchain access code) alerts the rest of the system to enemy intrusion. This immutable hardware/software information fingerprints/codes means that an enemy actor cannot masquerade as a smart node in the system to even gain access.

There are several large-scale digital twin systems now deployed and in development, such as the U.S. Air Force's (USAF) Tyndall Air Force Base (AFB) digital twin system (now under evaluation for large-scale deployment across the USAF). The Cities of Singapore and Shanghai have deployed very large-scale digital twin systems for "Smart City" management that monitor water and energy consumption and traffic flow and even help plan future development.

This incredible utility and value proposition, as well as the ability to deploy to currently existing sites via installation and deployment of edge node clusters for data management, is an ideal case study for hardening these systems via the implementation of blockchain-based cybersecurity, particularly at sites with critical infrastructure that are vulnerable to attack by criminals and other hostile actors.

TECHNOLOGY BRIEFING

Digital twin systems use a constellation of smart nodes (Figure 1) to visualize 3D assets and real-time data in large, synthetic environments that mirror a real-world area with a very high degree of accuracy. To achieve this unified experience, digital twin architecture must include and interconnect myriad software and hardware infrastructures. These smart node arrays integrate cybersecurity, systems integration, digital engineering, data management, platforms, analytics, and artificial intelligence (AI) to design and deliver comprehensive and valuable information to end users. Information flows generated by these systems include any information of value to the end user, such as logistics (power/water/supply chain), vehicle traffic, foot traffic, temperature (including individual building temperature), security infrastructure (including real-time, AI-driven personnel authentication or identification of threats), and any other bit of pertinent data that sensors can collect and report to the system. It can also be used as a planning tool for future changes to a city or installation by adding artificial planning data to test what changes will happen to the modeled installation.

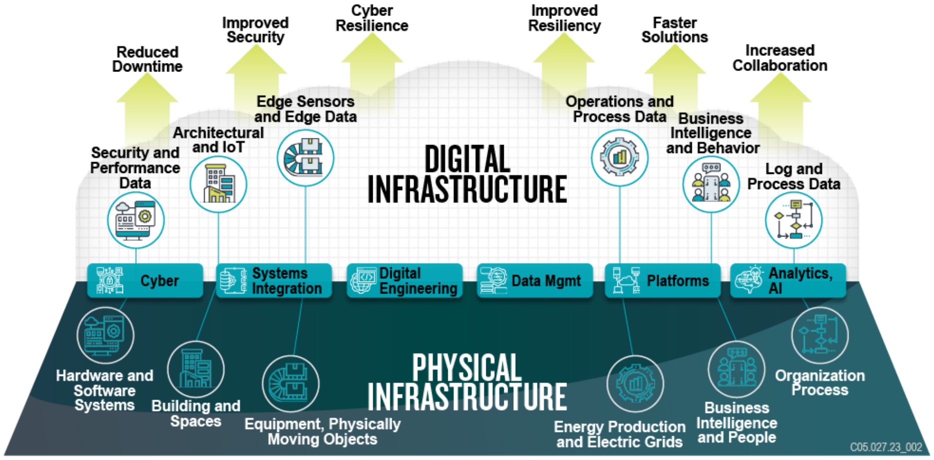
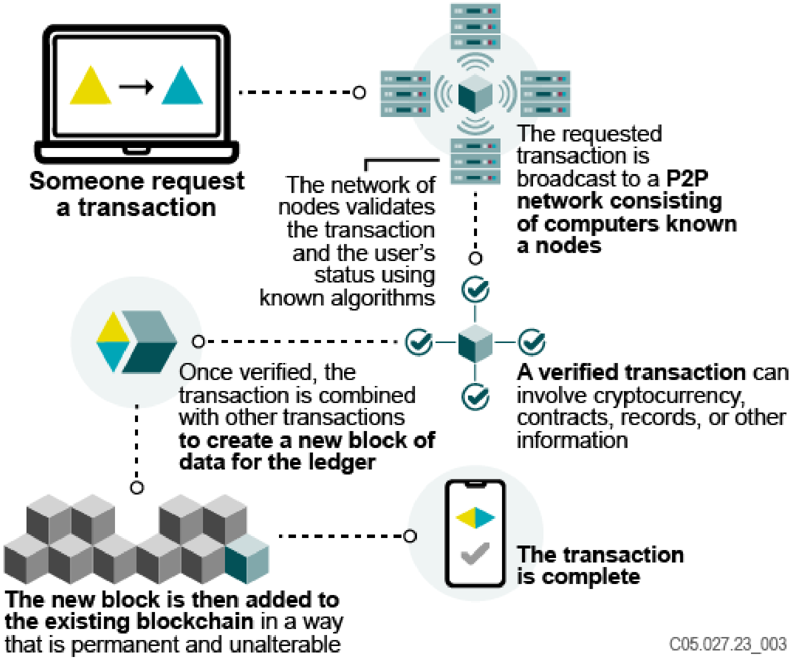


Figure 1

End users of digital twin systems must apply solutions that not only protect sensitive data, providing the right permissions and levels of access depending on the system and the datasets involved, but also create public trust. Digital twin systems integrate models, and datasets including proprietary information and personally identifiable information (PII) create unique challenges related to data ownership, security, and privacy.


Someone request a transaction

The requested transaction is broadcast to a **P2P network consisting of computers known a nodes**

The network of nodes validates the transaction and the user's status using known algorithms

Once verified, the transaction is combined with other transactions **to create a new block of data for the ledger**

A verified transaction can involve cryptocurrency, contracts, records, or other information

The new block is then added to the existing blockchain in a way that is permanent and unalterable

The transaction is complete

Figure 2

Blockchain (Figure 2) is a digital ledger technology that was created as the backbone of Bitcoin. However, blockchain is *not* inherently tied to cryptocurrency, and its dual-use applications are expanding through innovation. Once a blockchain transaction occurs, it cannot be altered without network consensus approval. Information is stored on a network of computers, or nodes, in the form of data records, or blocks. Nodes are connection points that store, send, and receive information across a network. If one node/database fails, redundancy across multiple nodes remains. Blockchain catalogs all operations related to an asset and publicly displays that information to every user with access to the network. If user identity is known, it is tracked throughout the transaction history, creating a perfect audit trail enabling robust (data) attribution. Blockchain is significantly impacting both commercial and government organizations. The usual linear value chain, where value is added in strict sequential order, is being replaced by a networked value chain where entities and the entire environment are networked together with automated code (e.g., smart contracts). In a networked value chain enabled by blockchain, there is a more efficient use of resources and process execution, which leads to cost savings and reductions in cycle times. In terms of the organizational structure, classical hierarchical layers may be replaced by a new model emerging from implementations of blockchain and other digital transformation technologies. Regarding tradeoffs of speed and performance using blockchain, there are current deployments of “lighter weight” blockchain for cyber purposes. There may be issues with very high bandwidth data transmissions that may or may not be pertinent to an installation of this type. Until each node in a digital twin cluster is tested for data density and interconnected performance, there will likely be adjustments made to the deployment of the blockchain solution on a case-by-case basis. Initial deployment at the highest point of need can be rolled out to work in conjunction with existing cybersecurity to validate the installation, reducing the cost and risk of deployment. Additionally, as it is a well-understood software solution, updating the software at the point of use should be straightforward on a regular basis.

PUFs are digital fingerprints that are generated by any physical electronic device. The tiny variances, even between individual silicon chips, create a unique output signature that can be recorded. Any change in the chip, power system, or any other component that interfaces with the edge node changes the PUF identification fingerprint and thus invalidates the PUF code. This PUF code creates a verifiable code that corresponds to a smart node, and if a bad actor modifies the node hardware in any way, the system PUF changes and is no longer accurate. This generated PUF code can be stored in a blockchain algorithm, creating an immutable record of the edge node hardware in a secure state that can then be used as part of a network authentication protocol. As PUFs are a relatively new technology, there are some uncertainties about PUF validity in temperature extremes and it will likely require some testing to ensure the PUF signature characteristics are not impacted by environmental conditions.

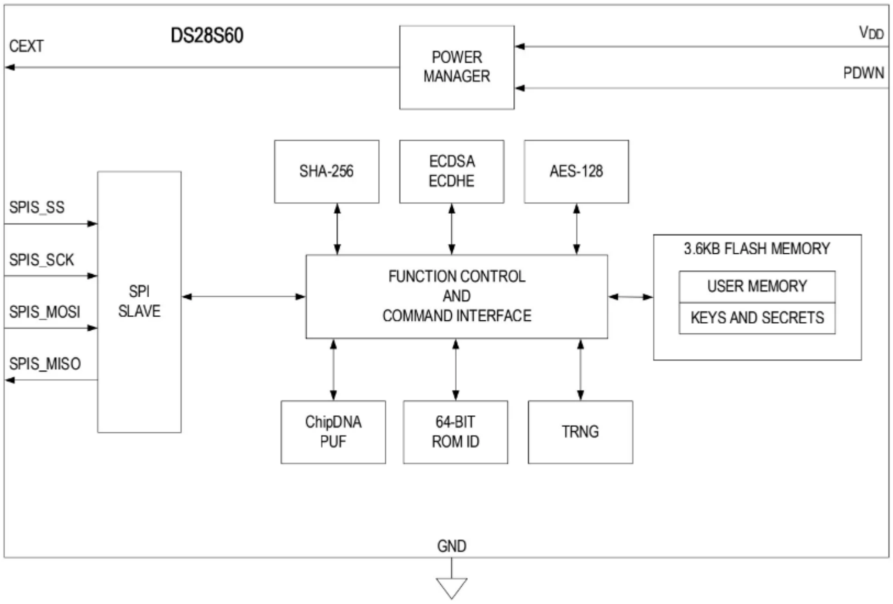


Figure 3

The diagram (Figure 3) to the left is an example of a PUF-supported architecture that could be deployed within a smart node in a digital twin cluster (in this case, a Maxim DS28S60 Coprocessor). This processor would then be able to respond to a challenge/response loop by providing its PUF to verify against a blockchain-secured PUF record for surety of hardware provenance. Unlike a conventional cryptographic approach, which uses a single stored key, PUFs work by creating and implementing an authentication step. Each PUF challenge will generate a response that is unique to the specific PUF, much like a fingerprint in a human, and therefore is a unique identifier that can be compared against the verified stored identifier and thus verified against tampering or substitution. When incorporated into a digital twin edge node cluster, this helps ensure that all operational nodes are not compromised at a hardware level, locking in the physical security of the smart nodes.

Smart (edge) nodes are a physical or virtual machine located at the edge of a network that can also act as a portal for communication with other computer nodes in cluster computing (e.g., digital twin). Smart nodes are also sometimes called gateway nodes or edge communication nodes. These arrays of computers are designed to interconnect and, due to their small size and wide deployment across a cluster, create a large cybersecurity "surface area" to protect. Edge computing can analyze data at the edge layer employing AI and machine learning (ML) algorithms. This makes devices smarter and able to generate quicker insights and feedback while intensifying their utility. Besides generating insights, these smart edge devices can collect data from IoT devices and share it with other edge servers over the networks for model training, analysis, and prediction. In the case of digital twin systems, these edge nodes can monitor logistical elements (like water, power, and supplies) and traffic (pedestrian, air, and road) and be deployed to mobile units (like security-carried, ATAK (Android Team Awareness Kit)-style systems and Augmented Reality systems).

TECHNICAL SOLUTION

Our solution is to deploy blockchain/PUF airlocks at every smart node in a cluster within a deployed digital twin environment to harden the communication physically and digitally into, out of, and through each node, thus optimizing data and hardware security.

Blockchain platforms are maturing quickly, and new lightweight blockchain platforms have been developed in the past few years. These blockchain platforms can be easily deployed in the edge devices, which have become more powerful computationally to handle the data and execute AI/ML models for real-time decisions. These lightweight blockchains will help ensure data consistency, traceability, and tamper-proofing, and protect data privacy in edge devices. Data stored in a blockchain consists of small amounts of data locked down with encryptions. When these “blocks” are “chained” together, nodes of the specific blockchain can easily view all data. The decentralized nature of the blockchain architecture helps to keep the security risks to an absolute minimum. There are many IoT companies (such as Helium, Xage Security, and Iota) that are using blockchain already in their products for many use cases. Hence, we believe that this solution is feasible and can be implemented. Data generated from the devices and network communications can be secured by storing blockchain transactions. These transactions can be validated by smart contracts, making the communication between devices more secure. Today’s secure standard protocols used in the IoT can be extended with blockchain application. Thus, blockchain will be an ideal choice to maintain privacy, security, and trust in the data stored in edge devices.

The following figure depicts a more generic blockchain-enabled edge computing architecture for securing the data in edge devices, such as those encapsulated within a digital twin cluster.

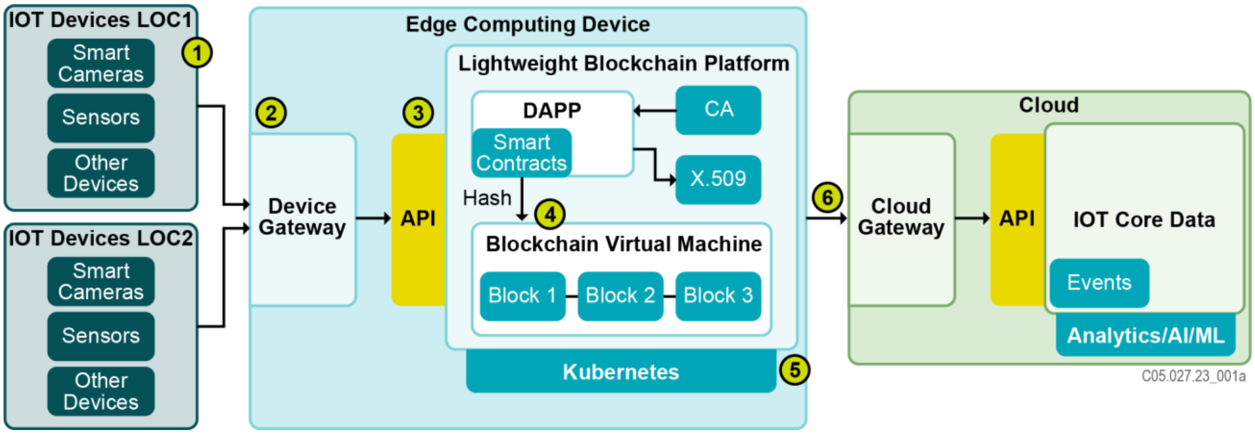


Figure 4

Proposed Lightweight Blockchain Architecture in Edge Devices Adds a Strong Security Layer for Data at Rest and in Transition

The following table shows the multiple layers of data flow and security can be applied at each layer of the edge device from IoT devices to the edge computing device and then to the cloud computing infrastructure.

Table 1. Proposed Blockchain Architecture Flow in Edge Devices

Step	Description
1	Data is generated in IoT device such as cameras, AR/VR sets, sensors, and digital twins.
2	IoT device invokes an application programming interface (API) through device gateway using MQTT communication protocol. Device gateway acts as a firewall and filters the data if needed before invoking API in the DApp deployed in the lightweight blockchain.

3	API invokes the x.509 certificate for authenticating smart devices. Once successfully authenticated, API invokes a smart contract that implements access control and creates the transactions in the blockchain.
4	Smart contracts validate the data and transactions are committed in the form of blocks with hashing on each transaction.
5	Lightweight Kubernetes engine can be used to run the DApps. Kubernetes provides innate security advantages and provides additional guardrails to secure applications and data.
6	Data from edge devices are transferred to the cloud through an asynchronous process by executing an API using MQTT protocol that in turn invokes a topic in the cloud for further analytical solutions.

Table 2 captures security and privacy properties that entities and methods will enforce in different tiers of edge device security using blockchain. As the table shows, the security of blockchain technology mainly stems from the use of hash functions to chain blocks to help ensure immutability, as well as the use of encryption and digital signatures to secure data.

Table 2. Security and Privacy Properties at Each Layer

Properties	Edge Device	Network	Storage
Identity and Authentication	Ledger of Transaction	Signatures	Block Number with Hash
Access Control	Policy Header and Transactions in Blockchain	Multiset Transaction	Block Number with Hash
Protocol and Network	Encryption	Encryption	Encryption
Privacy	Non-Private	PK or ID	Block Number With Hash
Trust	Predefined	Verification	Signed Hash of Data
Nonrepudiation	Encryption	Signatures	Signed Hash of Data
Policy Enforcement	Policy Header	PK Lists	Accounting
Authorization	Policy Header and Transactions in Blockchain	List of Keys	Accounting
Policy Enforcement	Medium	High	Low

Blockchain Risks and Mitigation Strategies

Although there are great benefits to using blockchain to secure the data at edge devices, there are security risks we should ensure are fully understood and mitigated to avoid potentially exposing the critical data to vulnerabilities, attack vectors. Because blockchain applications are diverse and nuanced, they are vulnerable to a wide variety of threats across multiple domains. It is imperative to proactively identify and address these risks by implementing proper governance, processes, and controls to formulate effective threat mitigation strategies. The below table captures the risks associated with blockchain and the mitigation strategies.

Table 3. Blockchain Risks and Mitigation Strategies

Domain	Description	Mitigation Strategies
Governance	Encompasses blockchain design, including specific parameters, protocols, or algorithms, and regulatory and management oversight guidelines or requirements (e.g., policies and procedures)	• Regular network audits • Training administrators on the latest security threats and how to mitigate them • Implementing disaster recovery plan • Keeping up-to-date software • Ensuring access control and user authentication measures

Infrastructure	Any blockchain functionality or capability independent of a data transaction on the blockchain: 1. Software Vulnerabilities 2. Protocol Management 3. Consensus Mechanism 4. Data Management 5. Interoperability	• Implementing firewalls, intrusion detection systems, and antimalware software • Implementing secure communication protocols, such as Transport Layer Security (TLS) or Secure Shell (SSH)
Data	Offchain information that is stored or transmitted in a computer-legible format and used to transact or interact on a blockchain network, or onchain data that are sourced from a blockchain network and treated as a source of truth for a business purpose: 1. Data Integrity 2. Access Rights 3. Blockchain Bloat 4. Nonstandard Transactions 5. Data Output 6. Out-of-Range Data 7. Orphan Address	• Authorized and permissioned client access to database, server, or parser application resources that transmit, compile, or translate data to create a blockchain transaction • Implementing advanced encryption algorithms that ensure security and tamper-proofing • Applying the latest encryption protocols Advanced Encryption Standard (AES), RSA, and Elliptic Curve Cryptography (ECC) • Strong processes to check the validity of a recipient's blockchain address when sending transactional information
Key Management	Management of public and private keys: 1. Entropy 2. Key/Protocol Security 3. Sharding 4. Multisig 5. Wallet Management 6. Hardware Security Module 7. Hardware Security Model Access	• Strong protection of the private and public keys • Sufficient key backup assistance • Proper physical and logical access controls for primary and backup keys • Proper keyholder grant and revoke policies and procedures • Strong two-factor authentication mechanisms • Use of encryption algorithms that are not widely recognized as providing strong encryption to store or transmit keys
Smart Contracts	Blockchain networks and other distributed-ledger technology that run virtual machines and decentralized code and allow for programmatic value transfer and recording of state and other transaction data: 1. Governance Risk 2. Design Risk 3. External Interaction Risk 4. Manipulation/Denial of Service Risk	• Ensuring the consensus protocol's security is critical to prevent malicious actors from manipulating blockchain data • Full unit testing • Smart contract security audit • Code uniqueness • Strict access controls

Blockchain Synergy with 5G, IoT, and Cloud Computing

- IoT and the cloud have given rise to big data, which can be processed with AI to enable new insights. Data collected and initially processed at the edge (IoT devices) will rely on 5G networks to transmit back to the cloud and be collected in data lakes. The monetization of this data encourages more IoT devices and increases the usage of 5G networks and cloud infrastructure.

- **Blockchain technologies underpin this process**, making data immutable and automating trust between parties to enable new, community-based business models. As was seen on the internet, these services will disrupt a substantial portion of the legacy economy.
- Although blockchain technology is far from mature, broad conceptual and technical underpinnings are taking shape, **accelerated via increasing investor participation across all four tech areas.**
- Areas like logistics have struggled due to lack of development in one or more of these four areas. Some of the use cases are awaiting new 5G networks, deployment of IoT devices, or improved AI. **Blockchain may spur development of these and help overcome technical gaps (AICPA & CIMA, 2021).**

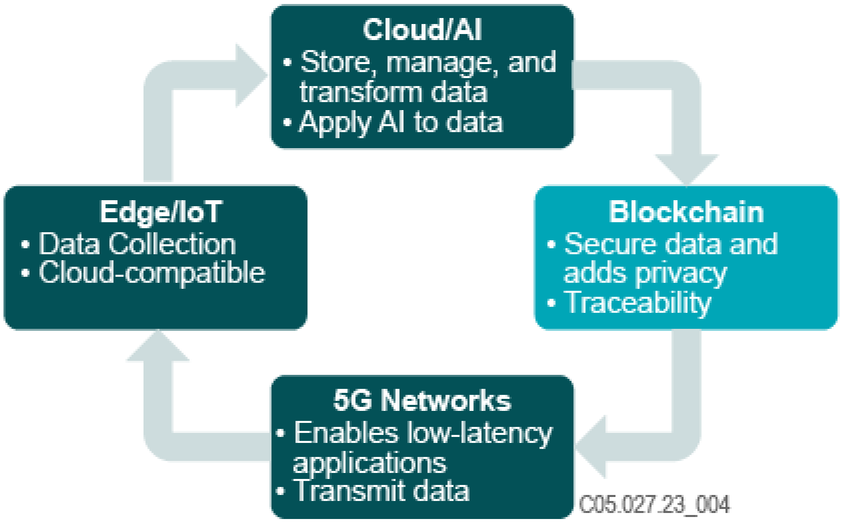


Figure 5

This synergy of technologies (figure 5) like cloud/AI, edge, blockchain, and 5G support offers a unique opportunity to deploy complex computing clusters that are optimized for operations such as digital twin but are hardened against cyberattack through the unique provisions of blockchain code. As these systems operate in gestalt, a unique cybersecurity solution (Hazra et al., 2022) is revealed that, along with existing Zero Trust policies, can be used to create tools for large-scale data organization and modeling that are unique to digital twin constructs. This, in turn, will make large-scale utilization of digital twin applications easier and safer to deploy.

AN EXAMPLE OF DIGITAL TWIN AND BLOCKCHAIN FOR CYBERSECURITY FUNCTIONS

The port has a massive concentration of shipping, surface traffic, pedestrian workers, and rail lines that create a unique multilevel problem of both control and cybersecurity. This makes for an ideal location to deploy a digital twin application for shipping management, site security, first responder, logistics, and homeland security purposes. This stream of dense traffic also makes it an ideal location for attack by hackers intent on disrupting our economy, smuggling, terrorism, or rerouting shipments for theft.

With much of global hacking now emanating from Pacific Rim nations such as China and North Korea, it is critically important to create a cybersecurity-hardened operating environment that can simultaneously aid in the command-and-control opportunities created using digital twin technologies.

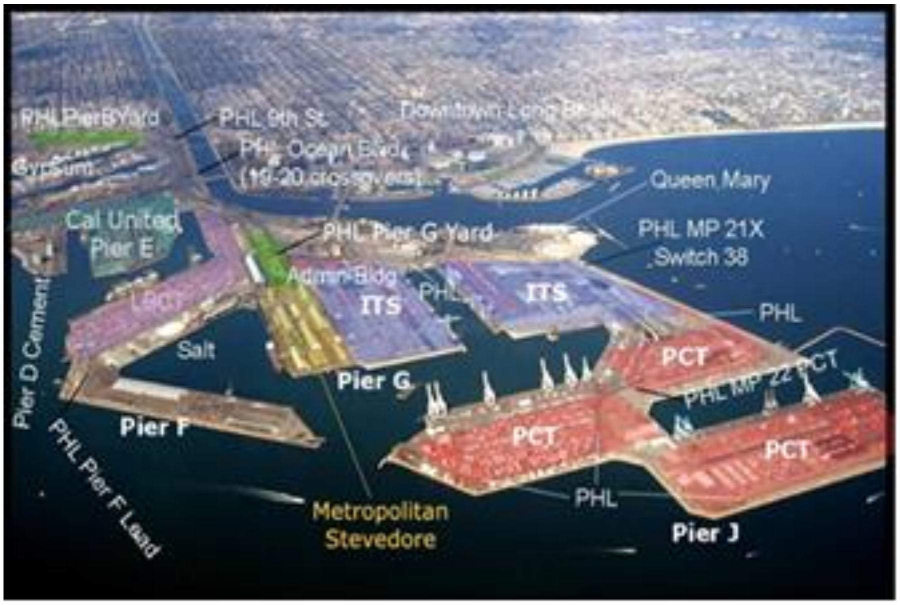


Figure 6

This image (Figure 6) depicts a typical large American port. At this location, roads and railways converge to move cargo to and from the terminal that continuously services a tremendous amount of cargo shipping vital to the U.S. Recently, during the COVID pandemic, shipping was massively disrupted at this facility, resulting in significant delays and increased operational costs to the entire country as well as our trading partners using the port (McNair, 2022). In the real-time digital twin application servicing the port facility, edge nodes across the facility continuously feed vital logistical information to the central server along with security alerts, traffic flows, and all pertinent data for analysis and action.

These clusters of smart nodes create an optimized flow of information mirroring all aspects of port operations. These edge nodes also create a large-scale vulnerability, increasing the “surface area” of the computer network that might be vulnerable to cyberattack. With each node being both independently operating but also communicating across the cluster, under normal circumstances a normal cyber solution would still leave the system vulnerable to penetration where a hacker accesses an individual node and then uses that access to gain access to the entire cluster.

The solution is to harden each node in the digital twin reporting cluster of edge nodes via blockchain. The immutable nature of the encapsulated data means that each edge node can be hardened individually, and using PUFs, each smart node can also be verified at a hardware level disallowing the substitution of a “dummy” hardware in the cluster, creating a mutually supporting hardware/software solution instantly verifiable through the verified immutability of blockchain-encapsulated data security. Each edge node would thus be airlocked in a cyber aspect, creating an array of mutually independent but instantly verifiably secure data nodes that can be assured of the provenance of the data, allowing full traceability of both the hardware and software from being compromised by hostile actors. Additionally, due to the real-time reporting nature of the digital twin system, the moment hostile action is attempted against any node in the system, it would instantly be reported to responding personnel for remediation.

This instant and hardened responsiveness to hostile action also creates a remediation against data disruption, allowing real-time management of port operations to be executed from a position of safety and efficiency, as all aspects of port operations are readily visible to users and a high level of confidence can be assumed to the supplied information from the edge nodes. This hardening also extends to mobile smart node users, such as first responders and security personnel who are using edge node devices to interface with the digital twin cluster to perform their functions without risk of compromise by hostile hackers.

CONCLUSION

Blockchain, in coordination with PUFs, offers the ability to radically harden cluster arrays, like digital twin installations, in a manner that dramatically reduces the ability for hackers to gain access into such large systems while being approachable for development in near-term timescales, due to their well-understood characteristics and their ability to deploy to current systems (as a software component) and to be forward-portable as next-generation quantum computing systems come online. Additionally, as blockchain is a mature technology, updating the installation characteristics should be a straightforward and well-understood effort, only impacted by the nature of the communications between the cluster nodes.

With many locations such as Singapore (Walker, 2023) and Helsinki (Kaupunki, 2023) already embracing digital twin technologies, it becomes more imperative to not only plan for implementation in the U.S., but to also plan on the best way to harden these points of critical infrastructure to cyberattack in a way that creates difficulty for bad actors to penetrate.

Finally, the inherent immutability of both blockchain and PUFs offers a particularly effective approach for simultaneously securing both the hardware and software elements of a cluster computing network like digital twin from compromise.

ABOUT THE AUTHORS

Michael Wikan is Creative Director for Booz Allen's Austin Immersive Group co-located with the Army Futures Command. He has 30 years of software design and development experience. His commercial software products have won numerous awards over the years including two British Awards for Film and Television Arts (BAFTA) and two products in the Smithsonian Collection.

Yugandhar Cindepalle is a certified blockchain expert for Booz Allen's Domestic Resiliency Group located in the Washington Metro Area. He has 25 years of software architecture, design, and development experience. He supported many federal agencies' information technology (IT) modernization efforts including DOD, Department of Homeland Security, and civilian agencies. He is leading the blockchain effort at Booz Allen and helping customers explore and adopt blockchain at the enterprise level.

REFERENCES

Capaccio, T. (2013). *Littoral Combat Ship Network can be hacked, Navy probe finds.* https://gcaptain.com/littoral-combat-ship-network-can-be-hacked-navy-probe-find/

Hazra, A., Alkhayyat, A., Adhikari, M. (2022). *Blockchain-aided integrated edge framework of cybersecurity for Internet of Things.* https://ieeexplore.ieee.org/abstract/document/9672722

AICPA & CIMA. (2021). *Blockchain risk: considerations for professionals.* https://www.aicpa-cima.com/resources/download/blockchain-risk-considerations-for-professionals

Port (https://polb.com/)

McNair, Sarah. (2022). *Tyndall AFB's Hololab debuts virtual gateway to installation of the future.* https://www.af.mil/News/Article-Display/Article/2971380/tyndall-afbs-hololab-debuts-virtual-gateway-to-installation-of-the-future/

Walker, A. (2023). *Singapore's digital twin – from science fiction to hi-tech reality.* https://infra.global/singapores-digital-twin-from-science-fiction-to-hi-tech-reality/

Kaupunki, H. (2023). *Helsinki's digital twin and city models.* https://www.hel.fi/helsinki/en/administration/information/general/3d/3d