Advances in Healthcare Information Technology
Workshop Report
November 14, 2017
Dulles, Virginia, USA

The NCOIC's Technical Council hosted a workshop on 14 November 2017 that brought together experts in the fields of blockchain applications and hyperconvergence infrastructure to discuss the feasibility of rapidly developing a solution for creating situational awareness of healthcare resources in disaster-recovery situations. This paper summarizes the information presented in the workshop.

Situational awareness involves the timely acquisition of knowledge about real-world events, distillation of those events into higher-level conceptual constructs, and their synthesis into a coherent context-sensitive view. Workshop speakers explored how convergent trends in video sensing, blockchain-secured communications and federated cloud standards can be leveraged to implement a solution for providing situational awareness to first responders.

The speakers had published their work in professional peer-reviewed journals, direct experience with implementing blockchain systems, or published work in hyperconvergence networks. Three speakers presented material related to blockchain applications and healthcare information systems. One speaker presented information on rapidly deployable federated networks for supporting data collection for situational awareness. Workshop participants discussed cybersecurity issues related to blockchain and federated networks. Technical problems related to interoperability of blockchains systems, wide area networks and network standards were also addressed. The following sections summarize the five keynote presentations.

Workshop participants included both NCOIC members as well as non-member experts. The information below does not represent an official or consensus position of the NCOIC's membership. The NCOIC is an industry led not-for-profit consortium established to promote secure interoperability and network centric operations. More information may be found at www.ncoic.org.

Blockchain in Healthcare Information Systems
Dr. Prithviraj Mukherji, Mukherji Consulting Inc., Centreville, Virginia, USA

In 2016-2017, NCOIC researched the idea of using a challenge team for developing a software/hardware system that utilizes blockchain software and rapidly deployable communication networks for situational awareness in disaster recovery situations. When Satoshi Nakamoto presented the simple idea for blockchains, little did he/she realize it would be applied across domains from diamond certification to banking systems to disaster recovery.

We have focused on healthcare applications for situational awareness. This implies obtaining information on availability of hospitals, clinics, and that healthcare providers capable of dealing with emergency disaster recovery.

Over the past five years, blockchain technology has been considered for healthcare information systems by a number of organizations in industry and government, such as the Office of the National

Coordinator/ Health and Human Services and Phillips Healthcare. Philips has launched a lab specifically aimed at blockchain research. The Hyperledger Healthcare Working Group features participants such as Accenture, Gem, Hashed Health, Kaiser Permanente and IBM. The MedRec platform developed by the Massachusetts Institute of Technology Media Lab and tested at Beth Israel Deaconess Medical Center is decentralized electronic medical records (EMR) management using blockchain technology to manage authentication, accountability and data sharing. Other instances include:

- Gem, a blockchain company, announced a partnership with Philips to build a private Ethereum blockchain for use in the development of enterprise healthcare applications.
- The American Enterprise Institute testified to Congress about the benefits of blockchain to health plans.
- The Office of the National Coordinator for Health Information Technology announced a blockchain challenge and received over 70 responses to its call for white papers on the technology and its potential use in health IT to address privacy, security and scalability challenges of managing electronic health records and resources.

Emphasis in all of these instances is on privacy, security and scalability. Blockchain technology inherently provides these three attributes by way of increasing confidentiality, availability and integrity of its records. For example, the user's choice of software applications, such as Epic, Evernote or Google Docs, is governed by third parties; Apple and Google maintain and curate (or in some cases, censor) the specific apps you're able to download.

Using blockchains, one entity will no longer have control over your medical records or notes; no one can modify or ban the app itself, temporarily taking all of your notebooks offline. Only the user can make changes, not any other entity. If all goes according to plan, Ethereum blockchains return control of the data in these types of services to its owner and the creative rights to its author. In theory, it combines the control that people had over their information in the past with the easy-to-access information that we're used to in the digital age. Each time you save edits, or add or delete content in notes, every node on the network makes the change.

Areas of potential application of blockchain technology in healthcare include: (see http://www.healthcareitnews.com/news/blockchains-potential-use-cases-healthcare-hype-or-reality)

- Master patient index. Blockchain could solve the challenge health systems have when their data sets get mismatched, or address the problem of duplicate records.
- Claims adjudication. Automated adjudication means being able to automatically take a claim and decide whether it's going to be paid or denied without manual intervention; 80% of claims are handled this way.
- Interoperability. This is the ability of two or more systems to exchange information and be able to use the information that's exchanged, working together across organizations to improve patient health.
- Longitudinal health records. Most of us go to our primary care provider roughly 54% of the time we engage with care. The other providers need to have a view of longitudinal records but don't have a complete view of our health history. What's needed is a clinical summary or view into what's going on with a patient, including labs, treatments and diagnoses.

NCOIC's approach is to develop a working prototype or proof of concept (POC) for demonstration purposes. Specifically, we will develop three types of user stories into demonstrable features. They are:

- Disaster recovery: provide situational awareness to providers and first responders.

- Sharing of patient information across secure, private or public networks on a global scale
- Healthcare payment systems

We will also develop non-user stories and provide hyperconvergence infrastructure (HCI) to support demonstration of POCs for private networks, public networks and “spikes,” including research on the initial coin offering for mining, bill payment and transfer of funds in “neuros” and “hdollars” across blockchain networks.

Such POCs will aid NCOIC’s role to provide government agencies with technical input on the interoperability of network and blockchain components during the initial planning and high-level design phases of a project’s lifecycle. The idea is to minimize risks associated with interoperability failures.

What is a blockchain?
Personal data, passwords and financial information are often stored on third-party computers, in clouds and servers owned by companies like Amazon, Facebook or Google. This provides a number of advantages; companies deploy teams of specialists to help store and secure this data, minimizing the costs that come with hosting and uptime. But there is also vulnerability. As we've learned in the case of Equifax, OPM and a number of other high-profile cases, a hacker or government can gain unwelcome access to your files without your knowledge by influencing or attacking a third-party service – i.e. they can steal, leak or change important information.

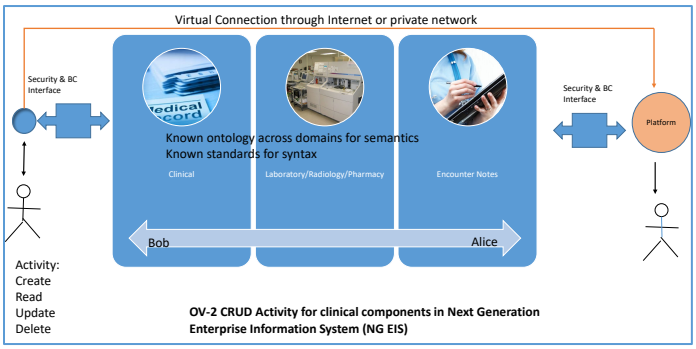
The internet was always meant to be decentralized. A movement has sprung up around using new tools, including blockchain technology, to help achieve this goal. Ethereum is one of the newest technologies to join this movement. A disruptor technology such as Bitcoin is aimed at PayPal and online banking. Ethereum’s goal is to use a blockchain to replace internet third parties that store data, transfer mortgages and keep track of complex financial instruments. Ethereum wants to be a “world computer” that would decentralize – and some would argue, democratize – the existing client-server model. In Ethereum, servers and clouds are replaced by thousands of so-called "nodes" run by volunteers from across the globe (thus forming a "world computer"). The vision is that Ethereum would enable this same functionality to people anywhere around the world, enabling them to compete to offer services on top of this infrastructure.

Implementation hurdles to adoption and use of blockchain technology include:
- Setting up network infrastructure for testing in development lab, test environment and production environment (need stubs and drivers, network infrastructure and software tools)
- Testing for scalability using increasing loads on CPU and network
- Obtaining buy-in from sponsor(s)
- Culture change within institutions requires overcoming inertia
- Dependencies exist on other software systems needed to support blockchain implementations, such as identity and access control systems, and security systems
- A lack of standards for blockchain systems interoperability

For over a year, we have designed and are developing a software application using blockchain software for situational awareness in disaster recovery situations. In addition to software, this application requires a communication network that can send and receive secure messages impermeable to hacking during transmission and subsequent storage in a database.

Sharing medical information globally in a secure and immutable manner can be implemented using local storage, a virtual communications network and distributed ledger technology (blockchains). A high-level operational view is presented in the following illustration for conceptualizing such a system of systems. It shows three types of medical information that can be shared across a global communications network by hypothetical users, Bob and Alice, who are geographically separated but connected by a virtual public (internet) or private (organization-dependent) communication network. They are:

- Clinical information related to conclusions from tests, images and diagnoses
- Laboratory tests, radiological imaging and pharmacy information related to a patient
- Provider-generated encounter notes after a patient visit with a provider



This illustration also shows the storage-related activities that must be considered after transmission has occurred. These include creating, reading and updating data. The delete operation in blockchain is forbidden so as to make blockchain records immutable. We call such a system of systems a Next Generation Enterprise Information System (NGEIS).

NGEIS can be useful for collecting and sharing situational awareness information. Blockchain technology assures that transmission and storage systems are secure and safe from hacking. Appropriate users within a pre-registered network of users can access the information on a need-to-know basis. For example, first responders can access critical information on safety and operations of buildings, such as hospitals, high rises, roadways, communication cell towers, etc.

In the event of a safety critical natural disaster, such as a hurricane or earthquake, cell towers are frequently damaged and communication networks are often rendered useless or are below acceptable performance criteria. In such situations, rapidly deployable virtual networks and cloud systems become imperative for rendering assistance to stricken people and systems.

Rapidly Deployable Communication Network
Dr. Kamesh Namuduri, University of North Texas, Denton, Texas, USA

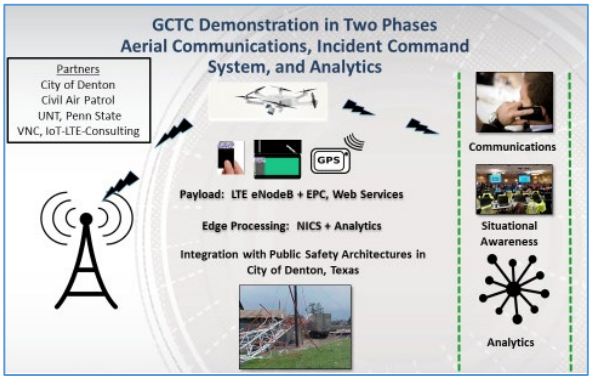
In the event of a major disaster such as a Category 4 hurricane or a massive tsunami, the likelihood of a functioning telecommunications network, such as the internet or a wireless-based local area network, is low to non-existent. For example, the magnitude 9.0 earthquake that struck eastern Japan in 2011 caused a massive tsunami. NTT, one of Japan's largest companies, sustained damage to its base-station equipment and 65,000 telephone poles in its network. As a result, mobile phone, laptop and landline performance was poor during the four days following the earthquake.

The advent of drone technology, coupled with long-lasting, battery-operated communication hardware, can be leveraged to implement a temporary communication network across the most damaged parts of the disaster zone. In a disaster recovery situation, first responders are forced to rely on outdated radios and networks as they look for survivors. Often, devices used by police officers cannot communicate with those used by firefighters, and walkie-talkies work only at short separation distances. If a

communication network can be rapidly deployed, then blockchain technology provides first responders with a system for secure communications across police and firefighter networks.

Emergency responders could use a fleet of drones to create a network of temporary base stations that operate from midair platforms. Using this network, which can be "meshed" for scalability reasons, responders from multiple agencies can share information. This network can then be used to increase situational awareness. It is interesting to note that the United States government in 2011 recognized the merits of such a system for communicating in disaster recovery situations. The idea did not gain any traction beyond merely noting the advantages of such a network.

In 2013, the University of North Texas, Massachusetts Institute of Technology's Lincoln Laboratory and Pennsylvania State University began designing a system that could be carried in the cargo hold of an ambulance or fire truck. First responders could launch the first drones carrying network base stations within minutes of arriving at a disaster scene, long before any telecom company could be there. With time passing, these drones would automatically reposition themselves as aerial base stations to maximize coverage. Several versions of a rapidly deployable drone-based network were tested over the last three years. The goal is to partner with private companies and public safety agencies around the world to help emergency responders stay connected during situations when it is a matter of life and death.



This figure shows the partners involved with testing drone-based networks in our research. The base tower shown in the lower left can also be drone carried in the event of its damage during a natural calamity. We envision a mesh of drone-located repositionable base towers providing communication capabilities over a disaster site.

In the United States, public safety agencies use more than 10,000 separate radio networks. Such disjointed networks present a hurdle for secure, interoperable communications. An example of the disastrous consequences of this disjointedness was evident in the World Trade Center destruction in 2001. Officials in New York City transmitted urgent instructions for emergency responders to evacuate the World Trade Center approximately 21 minutes before the second tower collapsed. Many police officers in the tower heard the dispatch and escaped, but firefighters in the tower never received the warning because their radios operated on different channels.

In the event of extreme damage to a telecommunications network, the current response is to dispatch technicians in trucks that haul temporary base stations to damaged tower sites. Additionally, mobile units, that are large trucks with base stations attached to antenna masts sticking out of the trucks, are dispatched. Among the drawbacks of this approach are:

- These trucks are expensive to maintain and store.
- Trucks can only go to places accessible by roads.
- Mobile-unit antennas cannot reach as high as a typical cell tower, so are susceptible to interference. This can have deadly consequences during disasters when call volumes have surged to 40 times the normal rate.
- It takes time to deploy multiple trucks (100s-1000s) to multiple places.

In contrast, there are several advantages to aerial communications systems that employ drones, including:

- These communication networks are less susceptible to interference.
- Drones can be automatically repositioned over areas where roads are inaccessible. One truck can deploy many drones (base stations), so recovery time is significantly decreased.
- Overall cost of maintenance is low, as the requirement for trucks is significantly decreased.
- A shared radio-channel frequency allows first responders from multiple agencies to exchange information using drone portable base stations with attached power supply and a digital database for containing the information.
- Blockchain technology for sending and receiving information ensures maximum security, confidentiality and integrity (immutability) of the messages during transmission, and storage in the database.

Our future work will include implementing a blockchain-based communication software application that can be loaded on smart devices and mobile units for use by first responders. Details of our drones, communication hardware, batteries and network technology can be found at *IEEE Spectrum* (North American), September 2017, pages 41-43.

Among the important considerations we had was to select base-station hardware that can be carried by drones weighing under 25 kg, a limit imposed by the U.S. Federal Aviation Administration. A 25 kg drone can carry a maximum payload of 2 kg. The product that best fits this requirement is GreenCell from Virtual Network Communications of Chantilly, Virginia.

Another important consideration was drone selection. Ideally, a drone should fly 10-12 hours before needing a recharge. CyPhy Works has a tethered drone that extends 150 meters from a power grid or generator. Under normal circumstances, this drone can stay up as long as it has access to its tether. In a disaster zone, this drone is tethered to a van carrying a generator and fuel. But if no roads are accessible, then this is not a viable option. Balloons were considered but rejected, as these are hard to reposition and hold in place during high winds. The choice was narrowed to the AR200 drone from Air Robot, a company in Arnsberg, Germany.

The final key consideration was the choice of a frequency that could be shared by first responders, without the risk of interference, interruption or channel crowding. Band 14 (700-800 megahertz) is reserved for use by public safety organizations. This band is managed by FirstNet, an independent authority within the U.S. Department of Commerce. Mobile phones programmed to work with Band 14 are available from Sonim Technologies in San Mateo, California.

Tests conducted over several years show that, with some additional modifications to GreenCell base stations, drone-based networks are a viable option for disaster recovery. The use of blockchain software for encrypting transmissions and storage in multiple locations each having a database is a secure and confidential system protected from hackers.

The final question is the cost of a drone-based network versus conventional commercial systems. A commercial drone capable of carrying a sufficient payload can cost as much as $100,000. A GreenCell base station costs tens of thousands. Currently, handheld mobile devices cost about $1,000 each. Over time, these costs should decrease. Drone-based communication systems are compact, affordable and capable of staying aloft for several hours at a time. Other groups developing similar technology include

Facebook and a research team from Ghent University in Belgium. The popularity of such systems are expected to grow.

Blockchain and its Application in Healthcare
Gautam Mohan and Varun Nagarajan, KrypC Corp., Bengaluru, India

Krypcore is a software application developed by KrypC Corporation to facilitate in an enterprise in the early adoption of blockchain technology for satisfying business requirements. An appropriate protocol is chosen from available frameworks (Hyperledger or Ethereum) for a software application for communicating "snackable" bytes of situational awareness information. A communications network will be required to support the information exchange. Here are some of the key features of blockchain technology and how Krypcore helps in the early adoption.

A blockchain is a distributed database that uses a procedure for maintaining a continuously growing list of data records. Such a blockchain database is hardened against tampering and revision, even by its operators. Key elements of blockchain include:

- Digital Signature. Authorization is achieved by a digital signature using an individual's private key.
- Visibility. Blockchain is a shared database that is transparent to all participants or a distributed database that can be cross verified for hash codes linked to individual blocks of data created.
- Validation. Blockchain-based software application checks for availability of assets, signature matching and tampering information.
- Block is a component of a blockchain that stores transaction information.
- Publish. All transaction information in the blockchain is published after validation and conformation.

Most blockchain applications have these five common elements in their operations; the resulting application is extremely robust and cannot be easily tampered with and/or hacked.

The most significant differences between traditional and blockchain databases are:

- Storage. Traditional databases can be centralized storage facilities. This allows a single point of failure in the database to make access to information unavailable if the server fails or is hacked, or is attacked by denial of service. This condition is considered a major vulnerability of centralized databases. Blockchain databases are served by multiple servers and data can be retrieved even if one is down.
- Participants who can control data ownership. Single databases or cloud storage facilities have a single-operator organization responsible for ensuring security and accessibility of the data. Blockchain databases are multiply owned and controlled.
- Transparency. In centralized traditional clouds or database systems, access can be restricted by the agent, who controls the storage. In blockchain databases, transparency is present across participants, who can view the information without access control by a single supervisory agent.
- Security. Traditional databases allow the data to be edited/deleted easily by the database administrator. Data cannot be edited/deleted even by the database administrator or other operators.

- Consensus. Decision-making authority for transactions lies with a single agent in traditional databases. In blockchain databases, transactions can only occur after consensus is reached among participants.

The reason for the recent interest in blockchain software can be attributed to perceived improvements in transaction verification efficiency and easier trust management in a trustless environment. These two features can result in cost savings. A recent article in *IEEE Spectrum* points out that more than half the world's largest companies are now researching blockchain technologies with the goal of integrating them into their products. (https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain*)*

If your current database cloud or system is managed by a single entity and this results in vulnerabilities of hacking, data integrity compromises and access issues, then blockchain databases are to be considered. Blockchain databases are controlled by multiple owners, who have unrestricted access to transparent transactions. If linear processing time for transaction to be settled or adjudicated is unacceptably long, then consider blockchain databases. If the need for transparency outweighs the need for privacy, then consider a blockchain database. For example, blockchain helps exchange information, such as "know our customer" (KYC) documents, with different parties transparently.

There are two primary kinds of blockchains, private and public. In a private blockchain:

- Read permissions may be restricted to an arbitrary extent.
- Write permissions are kept centralized to one system.
- Read access by all parties is not necessary, but auditability of blockchain is desirable.
- There is increased security and control over transactions.
- Participants with malicious intent can be restricted.
- An example is Ripple Labs cross-border remittance of money using blockchains.

In a public blockchain:

- Read permissions are public and available to anyone in the world.
- There is a completely decentralized system; consensus can be influenced by participants.
- Public readability and auditability are essential.
- There are less secure transactions due to anonymity and complete decentralization.
- No participant can be restricted from entering the blockchain.
- Likely applications include transactions of digital currencies like Bitcoin and Ether.

There are several issues with medical records sharing. Despite billion-dollar budgets for interoperable and shared records, federal agencies in the USA and Europe have not succeeded in making medical records patient centric and shareable among appropriate participants in the medical system. Some of these key issues include:

- Data sharing is limited due to lack of transparency and authenticity of documents.
- Critical data is not securely stored and is prone to hacking.
- There are many process-flow inefficiencies in creating the existing system of records.
- Auditing takes significant amounts of time, effort and cost due to forensic auditing methods required to audit the system of records.

Blockchain software provides multiple features for securing records, improving transparency, reducing process hops, and reducing the effort needed for auditing the system of records. It does this by the organic nature of the blockchain architecture, encryption, total transparency to member-initiated

transactions, and built-in audit characteristics of the system architecture. KrypC's software product, Krypcore, assists project developers and managers with bench-level development made easy.

Health WIZZ: My Healthcare in My Hands
Vikram Chauhan and Raj Sharma, Health Wizz Inc., Alexandria, Virginia, USA

Today, our health records are scattered all over the place, including hospitals, clinical, laboratories, pharmacies, paper records, data from wearables, genomic data and health insurance companies. Now imagine a world where every human being on the planet has access to their complete health record with them wherever they go.

Health Wizz is a software application that creates a comprehensive "womb-to-tomb" personal health record using distributed mobile platforms that leverage blockchain. The underlying technology supports transition from aggregation of records to sharing of medical records in a three-step process.

- Aggregation: scan paper records and information from patient portals.
- Organize and normalize data using standards where applicable.
- Share data using blockchain technology and distributed ledgers where the data stays with the user.

The resulting transformation creates a marketplace of health records. Pharmaceutical companies, research organizations, clinical studies, personalized medicine and insurance companies are potential customers in this newly realized scenario and constitute the marketplace. Users could share their data in exchange for less expensive insurance plans. A 2016 survey indicates that users are willing to share their medical data with health insurance companies in return for lower insurance costs (mHealth App Developer Economics study 2016, Research2Guidance). In response to the question "Do you think that mHealth app users would be willing to share health data with health insurance companies?" the response was 53% for cheaper plans, 18% for health recommendations, 15% said no, and 14% said they were willing to share for research purposes.

Two business models can potentially be applicable for marketing the Health Wizz application.

- Pharmaceutical companies pay a transaction fee to users when they purchase their medical records from users for research and precision medicine.
- Healthcare providers prescribe the Health Wizz application on discharge to reduce re-admission rates and manage chronic conditions. Incentives to providers to do this include a subscription fee per user given to the provider and a one-time fee to the provider to "white label" the application.

In the coming year, we are proceeding to develop these business models using demonstration versions of our Health Wizz application.

NIST/IEEE Joint Working Group on Cloud Federation: Current Status and Future Plans
Dr. Craig Lee, The Aerospace Corporation, El Segundo, California, USA

The goal of the National Institute of Standards and Technology (NIST)/Institute of Electronics and Electrical Engineers (IEEE) Joint Working Group (JWG) is to promote the development and adoption of cloud federation technologies to initially support the USA's national goals and economic

competitiveness. Ultimately, it is expected that such technologies will support a wide spectrum of secure collaboration capabilities across a wide spectrum of application domains across the world.

The NIST Public Working Group on Federated Cloud (PWGFC) and the IEEE P2302 Intercloud group had their kickoff meeting in August 2017. Each group has pre-identified contributions to their common goals. NIST PWGFC will develop a cloud federation vocabulary and conceptual model based on the scope and purpose of the JWG.

- PWGFC interim outputs will be communicated to the IEEE P2302 WG in real time.
- PWGFC final product will be one or more NIST special publications.

It is anticipated that many existing standards will be directly relevant to creating and managing federations. However, there may be gaps where federation-specific standards are needed. Hence, the IEEE P2302 Intercloud Working Group will develop one or more cloud federation-specific standards based on the scope and purpose of the JWG.

- PWGFC interim contributions will serve as input.
- Feedback on PWGFC vocabulary and conceptual architecture contributions will be provided to PWGFC in real time.
- P2302 initial output will be one or more federation-specific IEEE Standards.
- P2302 Standard(s) will be incorporated into the ISO/JTC1/SC#* to create an international standard(s).

Further details and information can be found on the references and links at right.

NIST Public Working Group on Federated Cloud (PWGFC) URL
- http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/FederatedCloudPWGFC

Request to be on NIST PWGFC Mailing List
- fedcloud@nist.gov

IEEE P2302 Intercloud Working Group URL
- http://sites.ieee.org/sagroups-2302/

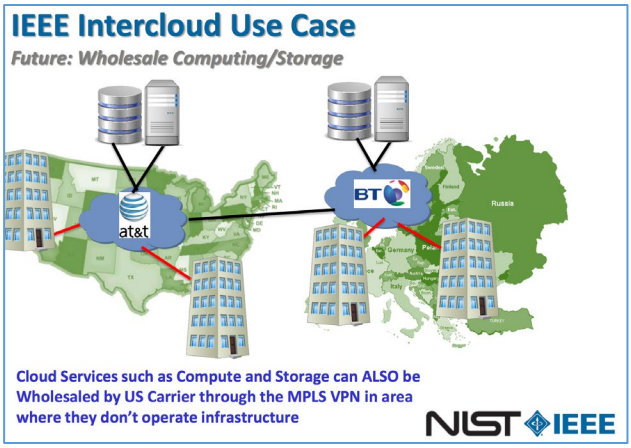
Request to be on IEEE P2302 Intercloud Working Group List
- STDS-P2302@ieee.org

The JWG-proposed model of intercloud federation allows for the integration of clouds at three levels of service on multiple servers providing multiple services. A conceptual service stack comprises three services in descending order on a vertical axis: these are Software as a Service (Saas), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Each of these three service levels can be integrated (federated) at any level in the system stack.

1. Arbitrary Application Level Federation applies to SaaS service level.
2. Platform Federation can be thought of as integration across PaaS.
3. Cloud Infrastructure Federation integrates IaaS level.

As such, cloud infrastructure federation can be seen as a special case of general service federation.

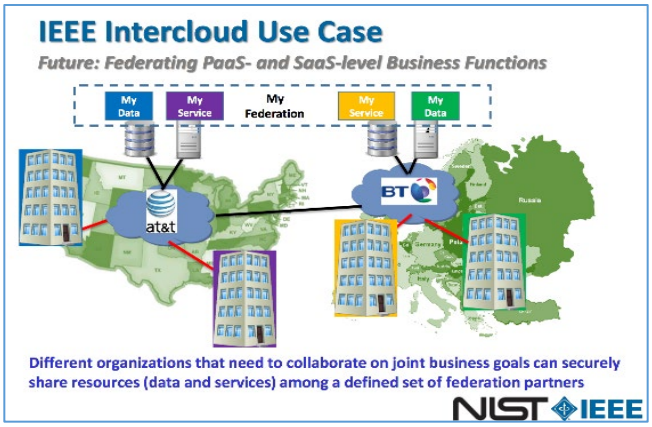
Prior work in the IEEE P2302 Intercloud WG concentrated on a *cloud wholesaling* use case across the globe, as seen in this high-level use case diagram (at right) of cloud federation across continents and "cloud wholesaling" of services.



Different organizations geographically separated across the continents that need to collaborate can securely share resources (data and services) among a defined set of federation partners.

This work on federation to support cloud wholesaling at the infrastructure level can be expanded to include PaaS- and SaaS-level functions, as illustrated below. It shows cloud federation across continents for arbitrary business functions. Here, business-level functions support the sharing of services or data among a defined set of federation participants can also be managed.

Potential collaborators that will enhance and broaden the proposed standard include:



- Open Research Cloud Alliance (ORCA): enable cloud-based "big-science" collaborations
- EU-Brazil Cloud Connect Project: Europe-Brazil collaboration of big data scientific research though cloud-centric applications
- OpenStack/Keystone: P2P federation agent design concept submitted, and 1-on-1 secure use for personnel
- Open Geospatial Consortium: federation presented as candidate technology for testbed 14
- European Grid Infrastructure: migrating grid based virtual organization infrastructure to OpenStack-based architecture
- Nectar: federation of 7-8 Australian institutions

This is just a short list "snapshot" in time. Additional collaborators are possible.

In summary, the success of the NIST/IEEE JWG efforts toward developing a conceptual model and vocabulary for hybrid clouds, "cloud wholesaling" and general federations will depend on engagement with stakeholders. There will a need to build prototypes for demonstrations, showing tangible benefits to potential users. Finally, the need to establish relationships with giant technology corporations, such as Amazon, Microsoft, Google and others, cannot be overstated.