Proceedings of the 2019 Winter Simulation Conference
N. Mustafee, K.-H. G. Bae, S. Lazarova-Molnar, M. Rabe, C. Szabo, P. Haas, and Y.-J. Son, eds.

A STUDY OF LIGHTWEIGHT DDDAS ARCHITECTURE FOR REAL-TIME PUBLIC SAFETY APPLICATIONS THROUGH HYBRID SIMULATION

Erik Blasch

Dynamic Data and Information Processing
Air Force Office of Scientific Research
875 N. Randolph Street
Arlington, VA22203, USA

Ronghua Xu
Seyed Yahya Nikouei
Yu Chen

Dept. of Electrical and Computer Engineering
Binghamton University, SUNY
P. O. Box 6000
Binghamton, NY 13902, USA

ABSTRACT

Utilizing the Dynamic Data Driven Applications Systems (DDDAS) framework for Smart Cities, a *Smart Public Safety (SPS) system* has become feasible by integrating heterogeneous computing devices to collaboratively provide public safety services. However, a service oriented architecture (SOA) is difficult to provide scalable and extensible services in a city-wide distributed Internet of Things (IoT)-based SPS system. Furthermore, traditional management and security solutions rely on a centralized authority, which can be the performance bottleneck or single point of failure. Inspired by the microservices architecture and blockchain technology, a *Lightweight IoT based Smart Public Safety (LISPS)* framework is proposed on top of a permissioned blockchain network. Through decoupling a monolithic complex system into independent sub-tasks, the LISPS system possesses high flexibility in the design process and online maintenance. The experimental results demonstrate the feasibility of the approach to provide a secured data sharing and access control mechanism.

1 INTRODUCTION

The Dynamic Data Driven Applications Systems (DDDAS) paradigm dynamically integrates modeling, instrumentation, and computation in a feedback control loop by combing data from simulations with that of real-time measurements (Fujimoto et al. 2018). DDDAS has shown promise in many areas (Blasch2018b)such as (1) *engineering*: aerospace, biomedical, civil, electrical and mechanical engineering, (2) *systems*: manufacturing, transportation, and energy design, (3) *science*: environmental, weather, and climate science, as well as (4) *decision support*: medical diagnosis and treatment, multimedia analysis, and cyber security evaluation.

The methods of generating simulated data from physical models (Fishwick 2016) with measurement models brings together conceptual and computer models using hybrid simulation to meet real-world challenges (Eldabi et al. 2016; Mustafee and Powell 2018). Methods for hybrid simulation include: Monte Carlo Simulation (MCS), Discrete-Event Simulation (DES), System Dynamics (SD) and Agent-based Simulation (ABS) (Brailsford et al. 2009; Katsaliaki and Mustafee 2011). Hybrid benefits (Mustafee et al. 2017) include the ability to process qualitative and quantitative analysis such as for image fusion (Zheng et al. 2012) and physics-based and human-derived information fusion (Hammoud et al. 2014). Current needs of hybrid simulation methods require verification and validation as well as systems understanding of the life cycle (Eldabi et al. 2018), especially in the age of cyber networking needs (Do et al. 2017) and big data (Onggo et al. 2018). Recent design choices in video application layer protocols (Sultana et al. 2019), IoT, and blockchain can benefit from hybrid simulations over numerous scenarios.

With the proliferation of Internet of Things (IoT) technology and DDDAS Smart City applications, a *Smart Public Safety (SPS) system* has become feasible by integrating heterogeneous computing devices to

978-1-7281-3283-9/19/$31.00 ©2019 IEEE

collaboratively provide public safety services. Normally, surveillance cameras are connected to the network to deliver the video to a central location or a server for further analysis. Although the internet infrastructure is getting more robust, the workload is getting more burdensome. Being aware of the growing demand for resources due to the ubiquitous deployment of networked static and mobile cameras, the surveillance community has made many efforts to offload the centralized cloud computing based system. Through processing video on-site or near-site at the edge computing devices, unnecessary latency and overhead on communication network can be significantly reduced. While the fog/edge computing paradigm promises solutions to address the shortcomings of cloud computing, such as communication delays and network security issues, it also introduces new challenges. It is not suitable to enforce management and security policies on a centralized authority basis, which suffers from the performance bottlenecks or single point of failures.

Instead of deploying the system as a monolithic unit as a traditional service oriented architecture (SOA), a *microservices architecture* divides a complex system into multiple atomic microservices that run independently on distributed computing platforms. Compared with a monolithic framework, the microservices architecture possesses many attractive features, such as good scalability, fine granularity, loose coupling, continuous development, low maintenance cost, and so on. These beneficial features allow microservices to be a prospective architecture to enhance SPS systems based on the edge computing paradigm. *Blockchain*, which acts as the fundamental protocol of Bitcoin (Nakamoto 2008), has demonstrated great potential to revolutionize the fundamentals of information technology (IT) due to many attractive properties, such as decentralization and transparency. A Decentralized Application (DApp), which is built on smart contract and deployed on blockchain network, performs pre-defined algorithms and agreement without relying on a third-party intermediary. Blockchain and a smart contract together are promising to provide a decentralized solution to enable a secured data sharing and access control in a SPS system.

Inspired by the microservices architecture and blockchain technology, a DDDAS hybrid-simulation inspired *Lightweight IoT (Internet of Things) based Smart Public Safety* (LISPS) framework is proposed on top of the permissioned blockchain network. By decoupling a monolithic complex system into independent sub-tasks, the LISPS system possesses high flexibility in the design process and online maintenance. Likewise, the blockchain-enabled decentralized security services provide a secured data sharing and access control mechanism.

The remainder of this paper is organized as follows: Section 2 discusses DDDAS control loops. Section 3 reviews the related works in microservices and blockchain. Section 4 overviews the high-level LISPS architecture and details of each part are described. Section 5 provides experimental results on real life scenarios, and Section 6 concludes the paper.

2 DYNAMIC DATA DRIVEN APPLICATIONS SYSTEMS (DDDAS)

Consider a public safety system. An environment model of a city can be constructed, but this has limited predictive value without knowledge of initial values, boundary conditions, inputs, parameters, and states (such as temperature and power). In order to make predictions, data is needed to estimate the unknown quantities. Although the city can be imaged at low resolution by a satellite, measurements by cameras with high resolution are expensive and limited in range, and image fusion results are subject to lighting conditions (Zheng et al. 2018).Therefore, the complete health of a city is difficult to obtain from detailed measurements over a large area.

In such a networked city scenario, it may be possible to use a model to guide and reconfigure the sensors so that the information content of the data is enhanced for the ultimate objective of predicting the power and service needs in a city (Liu et al. 2016). At the same time, the data collected by the sensors enhances the accuracy of the model by providing estimates of inputs, parameters, and states. The integration of on-line data with the off-line model creates a positive feedback loop, where the model judiciously guides the sensor selection and data collection, from which the sensor data improves the accuracy of the model.

2.1 DDDAS Concept for Simulation

DDDAS is a conceptual framework that synergistically combines models and data in order to facilitate the analysis and prediction of physical phenomena. In a broader context, DDDAS is a variation of adaptive state estimation that uses a *sensor reconfiguration loop* as shown in Figure 1 (Blasch 2018a). This loop seeks to reconfigure the sensors in order to enhance the information content of the measurements. The sensor reconfiguration is guided by the simulation of the physical process. Consequently, the sensor reconfiguration is *dynamic*, and the overall process is *data driven*.

The core of DDDAS is the *data assimilation loop*, which uses sensor data error to drive the physical system simulation so that the trajectory of the simulation more closely follows the trajectory of the physical system. The data assimilation loop uses input data if input sensors are available. The innovative feature of DDDAS paradigm is the additional *sensor reconfiguration loop*, which guides the physical sensors in order to enhance the information content of the collected data. The data assimilation and sensor reconfiguration feedback loops are *computational* rather than physical feedback loops. The simulation guides the sensor reconfiguration and the collected data, and in turn, improves the accuracy of the physical system simulation. The "model-based simulated data" positive feedback loop is the essence of DDDAS. Key aspects of DDDAS include the algorithmic and statistical methods that incorporate the measurement data with that of the high-dimensional modeling and simulation.

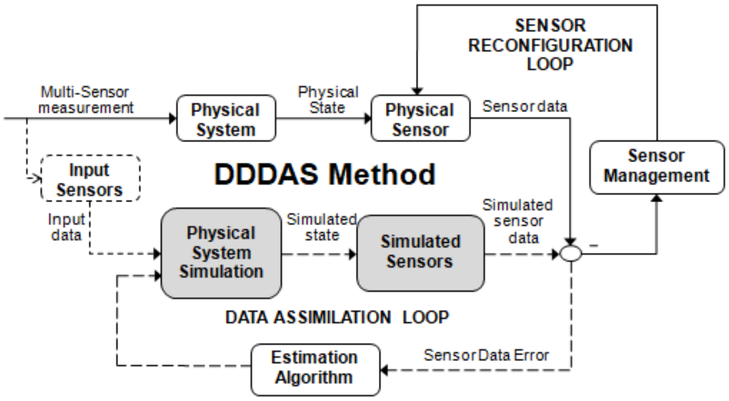

Figure 1: Dynamic data-driven application systems (DDDAS) feedback loop.

2.2 DDDAS Developments

The DDDAS concepts developed over two decades with the simulation methods (Blasch 2018a):

- *Scientific Theory* – Modeling and Analysis: enhancing the phenomenology of *science models* using measurement information and adaptive sampling incorporated into multiphysics, for example avionics (Imai et al. 2017) and smart cities (Fujimoto, et al. 2016).The use of simulation utilizes sensor measurements to confirm modeling, analysis, and usability of multi-physics techniques (de Villiers et al. 2015; Van Eeden et al. 2018).
- *Domain Methods* –Applications: utilizing data assimilation and multimodal analysis to that of control and filtering for methods of tracking (Dunik et al. 2015; Jia et al. 2016), situation awareness (Blasch et al. 2012b), and context-enhanced information fusion (Snidaro et al. 2016).
- *Architecture Design* – Systems and Software: designing scalable systems architectures and cyber network analysis, with recent efforts in cloud computing (Liu et al. 2014a). For example, the energy consumption of ground vehicles can be improved both locally for a car and globally for traffic (Neal et al. 2016). Another example of a *systems and software solutions* is a cloud-based system for real-time tracking of objects from Wide Area Motion Imagery (WAMI) streaming data (Wu et al. 2016). Finally, cloud computing for cyber physical systems (CPS) can manage the data streams

between CPS networked devices and those of sensors at the edge (Shekar et al. 2016). Li, Darema, and Chang (2017)combined these methods in a review of DDDAS support to a variety of applications such as distributed behavior model orchestration for cognitive internet of things (IoT).

3 MICROSERVICES AND BLOCKCHAIN FOR SMART PUBLIC SAFETY

There is a growing demand for human resources to interpret the live data streams from security cameras (Blasch et al. 2012a; Liu et al. 2014b; Chakravarthy et al. 2015). Numerous automated object detection algorithms have been investigated to atomize this process using statistical analysis (Fuse et al. 2017) or machine learning (ML) (Ribeiro et al. 2018) approaches. The ML methods are computationally expensive that are normally implemented for powerful cloud servers. For example, Wide Area Motion Imagery (WAMI) streams video from sensors back to the cloud for processing, which puts a heavy burden on the communication network (Wu et al. 2015; Wu et al. 2017). To reduce data transmission, it has been suggested to promote operators' awareness by using context (Blasch et al. 2014) or providing query languages (Aved et al. 2015). Further, approaches such as re-configuring the networked cameras (Piciarelli et al. 2016), utilizing event-driven visualization (Fan et al. 2017), and mapping conventional real-time images to 3D camera images (Wu 2015) improve the efficiency and throughput of the communication networks along with better detection rates.

Decentralized surveillance systems are more suitable in many mission-critical, delay sensitive tasks (Nikouei et al. 2018a). Recent developments of the edge hierarchy architecture enables real-time surveillance based on the fog computing paradigm (Mahmud et al. 2018).Many on-line and uninterrupted target tracking systems are proposed to meet the requirements of real-time video processing and instant decision making deployed at the edge (Mukherjee et al. 2018). Researchers also merged raw video streams from drones on near-site fog computing devices to reduce the amount of data to be outsourced to the cloud center (Chen et al. 2018).

A safety system focusing on object assessment can be constructed following the edge-fog-cloud hierarchy (Mouradian et al. 2017).The input surveillance video frame is given to an edge unit where low-level processing is performed, such as feature detection and object tracking(Blasch et al. 1998; Howard et al. 2017; Nikouei et al. 2018b; Xu et al. 2018d).The intermediate-level is in charge of action recognition, behavior understanding, and decision making like abnormal event detection, which is implemented at the fog stratum (Nikouei et al. 2018c; Nikouei et al. 2018d). Finally, the high-level is focused on historical pattern analysis, algorithm fine tuning, and global statistical analysis.

3.1 Microservices in IoT

A Service Oriented Architecture (SOA) is widely adopted in the development of application software in IoT and CPS environments (Butzin et al. 2017). The traditional monolithic architecture constitutes different software features in a single interconnected and interdependent application database. Owing to the tightly coupled dependence among functions and components, such a monolithic framework is difficult to adapt to new requirements for IoT-enabled systems, such as scalability, service extensibility, data privacy, and cross-platform interoperability (Du et al. 2014; Datta and Bonnet 2018). The *microservices architecture* allows functional units of an application to work independently with a loose coupling by encapsulating a minimal functional software module as a microservice, which can be individually developed and deployed. The individual microservices communicate with each other through a lightweight mechanism, such as an HTTP RESTful API or a message bus; asynchronously (Lu et al. 2017). Finally, multiple decentralized individual microservices cooperate with each other to perform the functions of complex systems. The flexibility of microservices enables continuous, efficient, and independent deployment of application functional units.

Because of fine granularity and loose coupling, the microservices architecture has been investigated in many smart solutions to enhance the scalability and security of IoT-based applications. Current IoT systems are advancing from "things"-oriented ecosystems to a widely and finely distributed microservices-oriented ecosystems (Datta and Bonnet 2018). An Intelligent Transportation Systems (ITS) that incorporates and combines the IoT approaches using the serverless microservices architecture has been designed and implemented to help the transportation planning for the Bus Rapid Transit (BRT) system (Herrera-Quintero et al. 2018). To enable a more scalable and decentralized solution for advanced video stream analysis for large volumes of distributed edge devices, a conceptual design of a robust smart surveillance system was proposed based on microservices architecture and blockchain technology (Nikouei et al. 2019). It aims at a scalable, decentralized and fine-grained access control solution.

3.2 Blockchain-enabled Security

Blockchain initially was used for new cryptocurrencies that perform commercial transactions among independent entities without relying on a centralized authority. Essentially, the blockchain is a public ledger based on consensus rules to provide a verifiable, append-only chained data structure of transactions. Due to the decentralized architecture, blockchain allows the data to be stored and updated distributively, which makes blockchain an ideal architecture to ensure distributed transactions among all participants in a trustless environment, like edge-based IoT networks.

Emerging from the intelligent property, a *smart contract* allows users to achieve agreements among parties through a blockchain network. By using cryptographic and security mechanisms, a smart contract combines protocols with user interfaces to formalize and secure relationships over computer networks (Szabo 1997). A smart contract includes a collection of pre-defined instructions and data that have been saved at a specific address of blockchain as a Merkle hash tree, which is a constructed bottom-to-up binary tree data structure. Through exposing public functions or application binary interfaces (ABI), a smart contract interacts with users to offer the predefined business logic or contract agreement.

The blockchain and smart contract enabled security mechanism for applications have been reported recently, for example, smart surveillance system (Nagothu et al. 2018),identification authentication (Hammi et al. 2018), access control (Xu et al. 2018a; Xu et al. 2018b),social credit system (Xu et al. 2018c), biomedical imaging data processing (Xu et al. 2019a), and space situation awareness (Xu et al. 2019b). Thus, blockchain and smart contract together are promising to provide a solution to enable a secured data sharing and access authorization in decentralized public safety systems.

4 SYSTEM ARCHITECTURE OF HYBRID SIMULATIONS FOR SPS

The proposed hybrid simulation for SPS framework follows the divide-and-conquer principle to functionally decouple the processes for public safety and system security. The computationally expensive processes are divided into multiple sub-tasks. Based on the microservices architecture, the proposed SPS system offers a completely decentralized solution where sub-tasks of a function are hosted by different hardware devices. An update or change of one service does not affect the operation of the entire system as long as it follows the same input and output relations. In the system design, a Docker container is adopted for the microservices architecture and the multi-layer SPS platform is implemented following the edge-fog-cloud computing paradigm. Figure 2 illustrates the proposed LISPS system architecture, which utilizes microservices-enabled private blockchain network to secure video stream services while providing secured data sharing. According to functionality and task completion, all containerized microservices are divided into four types and are deployed both at the edge and fog layer.

4.1 Smart Safety Applications Services

These microservices provide smart surveillance application functions, such as video stream processing, object detection and tracking, movement features extraction, anomalous behavior recognition, and safety alert actions. Real-time video streams are generated by cameras and transmitted to edge microservices for feature extraction. Lower level features are transferred to fog nodes for data aggregation and higher level analytic services, such as pattern recognition, behavior analysis and anomalous event detection (Wei et al. 2007). The light-weight Hyper Text Transfer Protocol (HTTP) webservice is deployed at the host and is responsible for data transfer between the edge and fog. Given different capacities of the host platform, the smart safety application services consist of edge services and fog services.

Smart Safety Application Services on the Edge: To reduce network communication latency and overload, raw video frames captured by cameras are processed by edge devices that conduct low-level feature extraction tasks, such as object detection and tracking. The key function of the features extraction task can be decoupled into multiple microservices that are deployed on a single or multiple edge devices and work cooperatively, as shown by Figure 2. In the object tracking and identification (Blasch et al. 2004) microservice, multiple frames are checked every second for pedestrian detection and feature extraction through a lightweight convolutional neural network (L-CNN) algorithm (Nikouei et al. 2018b;Nikouei et al. 2018e). Then, a tracker queue is maintained to track the detected objects within a bounding box, based on a lightweight, hybrid Kerman algorithm(Nikouei et al. 2018c). The Kerman tracker is optimized to have high accuracy in a restricted environment. Finally, movement-based features, such as the speed and direction changes, are extracted from the bounding box that the tracker gives for each object in each frame. The features for each object of interest are put into a dictionary format where the key is the object first detection time and the value consists of all the features. The extracted lower level feature is converted to a *JSON* string and transferred to the fog layer using HTTP protocol communication channel.

Smart Safety Application Services on the Fog: After extracted feature data have been merged by the fog platform through data streaming services, the higher-level feature contextualization and smart decision making for a surveillance system are available to support intelligent analytic functions. Prior to the decision making process, the data should be contextualized given significant factors, like the time of the day, the location of the camera, and the security level of the building which the camera is located in.

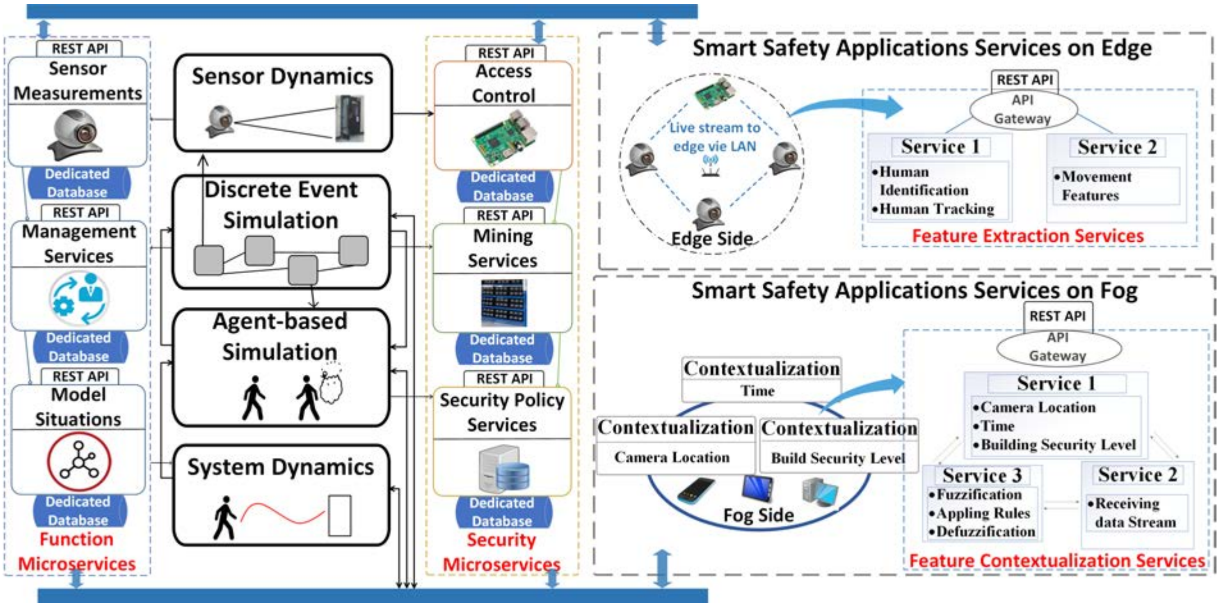

Figure 2: Systems architecture of hybrid simulations for SPS.

After the contextualization, the features of each detected human object in the frame are divided and separately processed by fuzzy logic microservices including fuzzification, applying fuzzy rules and defuzzification. Given pre-defined fuzzy logic rules, the suspicious activity level regarding a person anomaly is returned after defuzzification. According to a threshold defined by the system administrator based on the past experiences, the decision making is performed using a suspicious activity level (e.g., 80%) to output suspicious behavior recognition results. An email or a text massage is sent to the operator if suspicion level of an individual object is beyond the pre-set threshold.

4.2 Blockchain-enabled Security Services

In the LISPS system, security policy covers two main aspects: identity management and secured data accessing. An identity management mechanism ensures a new node enrollment process in the permissioned blockchain network. Only authorized participants could be recognized by entities of the network and perform blockchain services, such as mining blocks, sending transactions and deploying smart contracts. Compared to a public blockchain network, *the permissioned blockchain network* achieves higher efficiency in consensus operation, and more secure by limiting participants and clearly defining security policies. The secured data accessing service acts as a fundamental service pool, which includes three main clusters: access control services, security policies services and mining services. All the entities on the permissioned blockchain network are implemented as containers, which perform blockchain services independently on the host devices. The containerized microservices could be categorized as miners or non-mining nodes given the computation power of the host devices.

Utilizing the microservices architecture, the security policy functions are decoupled into multiple microservices and deployed on distributed computing devices. These decentralized security microservices work as a service cluster to offer a scalable, flexible, and lightweight data sharing and access control mechanisms for the LISPS system (Xu et al. 2019a). An entity registration process is performed by the registration microservices that associate entity's unique blockchain account address with a Virtual ID (VID). The identity authentication microservices expose RESTful APIs to other microservices-enabled providers for referring identity verification results.

The security microservices act as data and security service managers who deploy the smart contracts that encapsulate identity authentication and the access control policies. After the smart contracts have been deployed successfully on the blockchain network, they become visible to the entire network. The authorized participants could interact with smart contract through the Remote Procedure Call (RPC) interfaces. The access control microservices encapsulate access control model and perform access right validation during service granting process on smart surveillance service providers.

4.3 Hybrid Simulation Services

The hybrid simulation services combine multiple individual simulations models and techniques to implementation/model development stages of the simulation. The hybrid simulation offers an enhanced representation of the system including:

- *System dynamics simulation* is implemented as two microservices: sensor dynamics and system dynamics. The sensor dynamics simulation service could evaluate behavior of edge applications services and output estimates for sensor measurements and access control change. The system dynamics simulation services analyze the nonlinear behaviors of fog computing system to perform reconfiguration of the simulation models and system services.
- *Agent-based simulation (ABS)* controls the interactions of autonomous-given behavior recognition results from smart surveillance. Behavior recognition based on extracted lower features allows the assessment of individual objects in the video stream, and those individual agents will be analyzed by agent-based simulation to generate estimate for discrete event simulation.
- *Discrete-event simulation(DES)* combines estimates from agent-based model and a discrete sequence of events in time to model the operation of system. The event algorithm analyzes those multiple objects and assesses an event scenario during a certain period of time. In a discrete-event simulation, the event could refer to actions of a sensor or behaviors of object in video. The discrete-event simulation estimates coordinate agent-based services for improving accuracy.

5 HYBRID SIMULATION SERVICES RESULTS

A concept-of-proof prototype system has been implemented on a real physical network environment including a smart safety application and blockchain-enabled security services. The DES and ABS microservices cooperate with each other under close feedback loop to assistant system services. The smart safety applications are decoupled as multiple microservices that are developed as Docker images, and are deployed both on fog and edge computing platform. Two types of SBCs: a TinkerBoard and a Raspberry PI 3 model B+, act as edge computing in test system. The Tinker Board has 1.8 GHz ARM-based RK3288 SoC and 2 GB LPDDR3 dual-channels. The Raspberry PI 3 carries a 1.4 GHz CPU, which is a Cortex-A53 (ARMv8) 64-bit SoC, and a 1 GB of LPDDR2 memory. Both have an ARM-based CPU that makes it easier to deploy a Docker image based on the CPU architecture on both. The characteristic of low power consumption along with the small size and portability makes the SBCs the major candidates for edge processing. A laptop is adopted as the fog node, which has a 8-th generation Intel core i7 processor @3.1GHz with 4 physical cores and 16 GB of DDR4 memory.

Using the video processing, blockchain, and container-based systems; we augment the contextualization models of both the quantitative (processing needs) and the qualitative (social needs) for the system. Preliminary results of using the hybrid simulation within the *LISPS* framework demonstrate that the system performs in real time. Figure 3 shows that the processing on the edge units is utilized at 80%. Figure 4 shows the advantage of the hybrid simulation as the dynamic prediction models, agent-based approach to container use, and simulations results direct the fog services which reduces the processing time for the video analytics between video frames 10-25.

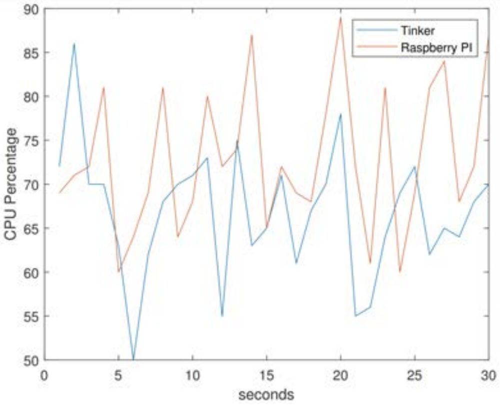

Figure 3: CPU usage percentage in the edge units.

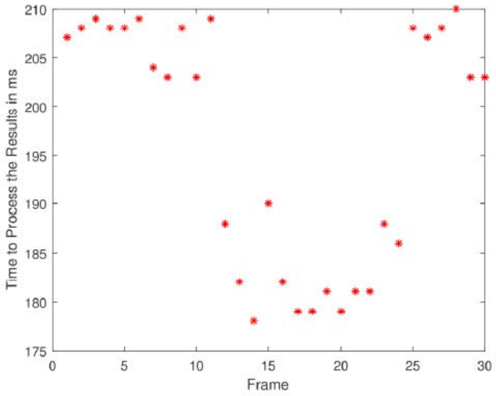

Figure 4: Process time on the fog node.

The permissioned blockchain-enabled security services network includes two miners deployed on a laptop and four miners distributed on four desktops. Each miner uses one CPU core. Two desktop and four Raspberry PIs are non-miners to run security microservices. The security microservices are developed as Docker containers providing both Go-Ethereum as a client application to interact with blockchain network and Flask-based webservice to handle security service request from user. To evaluate the performance, a service access experiment is carried out on a physical network environment which includes 3 Raspberry PIs and 2 desktops. One Raspberry PI works as a client to send service request, while server side is SPS service provider, which has been both hosted on edge (Raspberry PI) and fog (desktop) nodes. A blockchain enabled capability based access control (BlenCAC) scheme (Xu et al. 2018a; Xu et al. 2018b) is selected to enforce the access control policies. Figure 5 shows the computational overhead introduced by BlendCAC process. The entire executing time of the access control process is 42.4 ms (41.8 ms + 0.1 ms + 0.5 ms) on the edge device and 14.5 ms (14.2 ms + 0.1 ms + 0.2 ms) on the fog node.

To evaluate the overall network latency incurred by the microservices architecture, a comprehensive test has been performed on two service architectures: the microservices architecture (Micro App) and the monolithic framework (Mono App). Figure 6 shows the overall network latency incurred and compares the execution time of the BlendCAC and a benchmark without any access control enforcement on two service architecture. Considering the scenarios without access control enforcement, microservices and the monolithic framework have almost the same performance both on edge (51.3 ms vs. 55.4 ms) and fog platform (43.8 ms vs. 50.4 ms). However, when it comes to BlendCAC scenario, the experiments on two architectures show different communication latencies between the fog and edge platforms. Although microservices incurs more network latency, which is 73.6 ms (133.5 ms - 59.9 ms) on the fog side and 6.8 ms (147.1 ms - 140.3 ms) on edge side, it still brings benefits to the distributed IoT-based system, such as loosely coupled dependence, easy service deployment, and cross-platform interoperability.

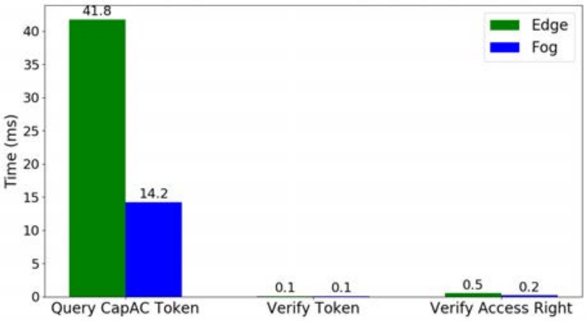

Figure 5: Process time of BlendCAC.

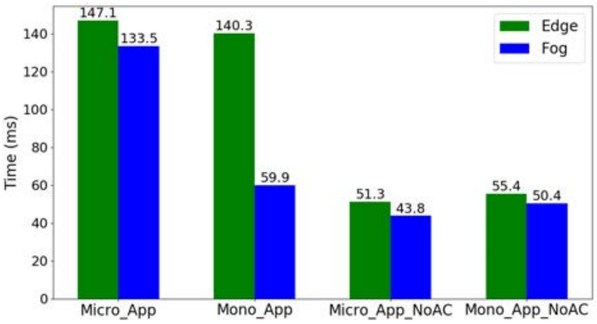

Figure 6: Network latency of BlendCAC.

6 CONCLUSIONS

Fundamental basic research in DDDAS is gathered from, and contributes to scientific applications, mathematical foundations, and infrastructure architectures. Specifically, DDDAS includes: (1)*theory*(e.g., estimation); (2)*methods*(e.g., image computing for situation evaluation); and (3)*design* (situation awareness through contextual assessment). Likewise, to bring together these services, a hybrid simulation approach was developed to enhance the *Lightweight Internet of Things (IoT) based Smart Public Safety (LISPS)* framework. Preliminary results show promise. Future work includes enhancing the discrete event and agent-based simulations to reflect the safety scenarios. The simulation enhancements with the real-world testing would afford methods to detect a more diverse set of behaviors, develop normalcy models for anomaly detection, and enhance user interaction through a user defined operating picture (UDOP) interface (Blasch 2013) for decision making (Blasch et al. 2011).

ACKNOWLEDGMENTS

The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Government.

REFERENCES

Aved, A. J. and E. P. Blasch. 2015. "Multi-INT Query Language for DDDAS Designs". *Procedia Computer Sci.* 51:2518–2532.

Blasch, E. 2013. "Enhanced Air Operations using JView for an Air-ground Fused Situation Awareness UDOP". *IEEE/AIAA Digital Avionics Systems Conference*, October 6th-10th, Syracuse, NY, USA, 5A5-1-5A5-11.

Blasch, E. 2018a. "DDDAS Advantages for High-Dimensional Simulation". In *Proc. of the 2018Winter Simulation Conference,* edited by M. Rabe, A. A. Juan, N. Mustafee, A. Skoogh, S. Jain, and B. Johansson,1418-1429. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc..

Blasch, E., E. Bosse, and D. A. Lambert. 2012a. *High-Level Information Fusion Management and Systems Design*. Norwood, MA: Artech House.

Blasch, E. R. Breton, P. Valin, E. Bosse. 2011. "User Information Fusion Decision Making Analysis with the C-OODA Model". *International Conference on Information Fusion*, July 5th -8th, Chicago, IL, USA, 2082-2089.

Blasch, E. and L. Hong. 1998. "Simultaneous Feature-based Identification and Track Fusion". *IEEE Conference on Decision and Control* (Cat. No. 98CH36171), December 16th-18th, Tampa, FL, USA, 1, 239–244.

Blasch, E., J. Nagy, A. Aved, W. D. Pottenger, M. Schneider, R. Hammoud, E. K. Jones, A. Basharat, A. Hoogs, G. Chen, D. Shen, H. Ling. 2014. "Context Aided Video-to-Text Information Fusion". *IEEE International Conference on Information Fusion*, July 5th-8th, Salamanca, Spain, 1–8.

Blasch, E., S. Ravela, and A. J. Aved (eds.). 2018b. *Handbook of Dynamic Data Driven Applications Systems.* Springer, Heidelberg, Germany.

Blasch, E., G. Seetharaman, K. Palaniappan, H. Ling, and G. Chen. 2012b. "Wide-Area Motion Imagery (WAMI) Exploitation Tools for Enhanced Situation Awareness". *IEEE Applied Imagery Pattern Rec. Workshop*, October 9th-11th, Washington, DC, USA, 1-8.

Blasch, E. and C. Yang, 2004. "Ten Methods to Fuse GMTI and HRRR Measurements for Joint Tracking and Identification". *International Conference on Information Fusion*, July 7th-14th, Stockholm, Sweden, 1-8.

Brailsford, S. C., P. R. Harper, B. Patel, and M. Pitt. 2009. "An Analysis of the Academic Literature on Simulation and Modelling in Healthcare". *Journal of Simulation* 3(3):130-140.

Butzin, B., F. Golatowski, and D. Timmermann. 2016. "Microservices Approach for the Internet of Things". *International Conference on Emerging Technologies and Factory Automation (ETFA)*, Sept 6th-9th, Berlin, Germany, 1–6.

Chakravarthy, S., A. Aved, S. Shirvani, M. Annappa, and E. Blasch. 2015. "Adapting Stream Processing Framework for Video Analysis". *Procedia Computer Science* 51:2648-2657.

Chen, N., Y. Chen, Y. You, H. Ling, P. Liang, and R. Zimmerman. 2016. "Dynamic Urban Surveillance Video Stream Processing using Fog Computing". *IEEE International Conference on Multimedia Big Data (BigMM)*, April 20th -22nd, Taipei, Taiwan, 105–112.

Datta, S. K. and C. Bonnet. 2018. "Next-generation, Data Centric and End-to-end IoT Architecture based on Microservices". *IEEE International Conf. on Consumer Electronics-Asia(ICCE-Asia)*, June 24th-26th Jeju, South Korea, 206–212.

de Villiers, J. P., W. D. van Eeden, W. A. J. Nel, K. H. Kloke, and E. Blasch. 2015. "A Comparative Cepstral based Analysis of Simulated and Measured S-band and X-band radar Doppler Spectra of Human Motion". *IEEE Radar Conference*, Oct. 27th-30th, Johannesburg, ZAF,283-288.

Do, C. T., N. H. Tran, C. Hong, C. A. Kamhoua, K. A. Kwiat, E. Blasch, S. Ren, N. Pissinou, and S. Iyengar. 2017. "Game Theory for Cyber Security and Privacy". *ACM Computing Surveys*, 50(2), Article 30, 1-37.

Du, L., M. Yi, E. Blasch, and H. Ling. 2014. "GARP-Face: Balancing Privacy Protection and Utility Preservation in Face De-identification". *IEEE International Joint Conference on Biometrics,* Sept. 29th-31th, Clearwater, FL, USA, 1-8.

Dunik, J., O. Straka, M. Simandl, and E. Blasch. 2015. "Random-point-based Filters: Analysis and Comparison in Target Tracking". *IEEE Transactions on Aerospace and Electronic Systems* 51(2):1403-1421.

Eldabi, T., M. Balaban, S. Brailsford, N.Mustafee, R. E. Nance, B. S. Onggo, and R. G. Sargent, 2016. "Hybrid Simulation: Historical Lessons, Present Challenges and Futures". In *Proceedings of the 2016 Winter Simulation Conference*, ed. by T. M. K. Roeder, P. I. Frazier, R. Szechtman, E. Zhou, T. Huschka, and S. E. Chick, 1388-1403, Institute of Electrical and Electronics Engineers, Inc.

Eldabi, T., S. Brailsford, A. Djanatliev, M. Kunc, N.Mustafee, and A. F. Osorio. 2018. "Hybrid Simulation Challenges and Opportunities: A Life-cycle Approach". In *Proceedings of the 2018 Winter Simulation Conference*, ed. by M. Rabe, A. A. Juan, N. Mustafee, A. Skoogh, S. Jain, and B. Johansson, 1500-1514, Institute of Electrical and Electronics Engineers, Inc.

Fan, C.-T., Y.-K. Wang, and C.-R. Huang. 2017. "Heterogeneous Information Fusion and Visualization for a Large-scale Intelligent Video Surveillance System". *IEEE Transactions on Systems, Man, and Cybernetics* 47(4): 593–604.

Fishwick, P. A. 2016. "Learning Simulation Models through Physical Objects". In *Proceedings of the 2016 Winter Simulation Conference*, ed. by T. M. K. Roeder, P. I. Frazier, R. Szechtman, E. Zhou, T. Huschka, and S. E. Chick, 1559-1570, Institute of Electrical and Electronics Engineers, Inc.

Fujimoto, R. M., J. Barjis, E. Blasch, W. Cai, D. Jin, S. Lee, and Y-J Son. 2018. "Dynamic Data Driven Application Systems: Research Challenges and Opportunities". In *Proceedings of the 2018Winter Simulation Conference,* edited by M. Rabe, A.A. Juan, N. Mustafee, A. Skoogh, S. Jain, and B. Johansson, 664-678. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Fujimoto, R. M., N. Celik, H. Damgacioglu, M. Hunter, D. Jin, Y-J Son, and J. Xu. 2016. "Dynamic Data Driven Application Systems for Smart Cities and Urban Infrastructures". In *Proceedings of the 2016 Winter Simulation Conference,* edited by T. M. K. Roeder, P. I. Frazier, R. Szechtman, E. Zhou, T. Huschka, and S. E. Chick, 1143-1157. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc..

Fuse, T. and K. Kamiya. 2017. "Statistical Anomaly Detection in Human Dynamics Monitoring using a Hierarchical Dirichlet Process Hidden Markov Model". *IEEE Transactions on Intelligent Transportation Systems* 18(11): 3083-3092.

Hammi, M. T., B. Hammi, P. Bellot, and A. Serhrouchni. 2018. "Bubbles of Trust: A Decentralized Blockchain-based Authentication System for IoT". *Computers & Security* 78: 126–142.

Hammoud, R. I., C. S. Sahin, E. P. Blasch, B. J. Rhodes, and T. Wang. 2014. "Automatic Association of Chats and Video Tracks for Activity Learning and Recognition in Aerial Video Surveillance," *Sensors* 14: 19843-19860.

Herrera-Quintero, L. F., J. C. Vega-Alfonso, K. B. A. Banse, and E. C. Zambrano. 2018. "Smart ITS Sensor for the Transportation Planning based on IoT Approaches using Serverless and Microservices Architecture". *IEEE Intelligent Transportation Systems Magazine* 10(2): 17-27.

Howard, A. G., M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, and H. Adam. 2017. "Mobilenets: Efficient convolutional neural networks for mobile vision applications". arXiv preprint arXiv:1704.04861.

Imai, S., E. Blasch, A. Galli, F. Lee, and C. A. Varela. 2017. "Airplane Flight Safety Using Error-Tolerant Data Stream Processing". *IEEE Aerospace and Elecronics Systems Magazine* 32(4):4-17.

Jia, B., K. D. Pham, E. Blasch, D. Shen, Z. Wang, and G Chen. 2016. *"*Cooperative Space Object Tracking using Space-based Optical Sensors via Consensus-based Filters". *IEEE Transactions on Aerospace and Elec. Sys.,* 52(3):1908-1936.

Katsaliaki, K. and N. Mustafee. 2011. "Applications of Simulation Research within the Healthcare Context". *Journal of the Operational Research Society* 62(8): 1431-1451.

Li, C-S., F. Darema, and V. Chang, 2017. "Distributed Behavior Model Orchestration in Cognitive Internet of Things Solution". *Enterprise Information Systems* 12(4): 414-434.

Liu, B., E. Blasch, Y. Chen, A. J. Aved, D. Shen, and G. Chen. 2014a. "Information Fusion in a Cloud Computing Era: A Systems-Level Perspective". *IEEE Aerospace and Elect Systems Magazine* 29(10): 16-24.

Liu, B., Y. Chen, E. Blasch, K. Pham, D. Shen, and G. Chen, 2014b. "A Holistic Cloud-Enabled Robotics System for Real-Time Video Tracking Application". *Future Information Technology, Lecture Notes in Electrical Eng.*, 276:-468.

Liu, X., D. Jin, C. W. Lee, and J. C. Moon. 2016. "CONVENUS: Congestion Verification of Network Updates in Software-defined Networks". In *Proc. of the 2016 Winter Simulation Conference*, ed. by T. M. K. Roeder, P. 1. Frazier, R. Szechtman, E. Zhou, T. Huschka, and S. E. Chick, 1131-1142, Institute of Electrical and Electronics Engineers, Inc.

Lu, D., D. Huang, A. Walenstein, and D. Medhi. 2017. "A Secure Microservice Framework for IoT". *IEEE Symposium on Service-Oriented System Engineering (SOSE),*April 6th-9th, San Francisco, CA, USA, 9–18.

Mahmud, R., R. Kotagiri, and R. Buyya. 2018. "Fog Computing: A Taxonomy, Survey and Future Directions". *Internet of Everything*, edited by B. Di Martino, KC. Li, L. Yang, A. Esposito, 103–130. Singapore:Springer.

Mouradian, C., D. Naboulsi, S. Yangui, R. H. Glitho, and M . J. Morrow. 2017. "A Comprehensive Survey on Fog Computing: State-of-the-art and Research Challenges". *IEEE Communications Surveys & Tutorials* 20(1): 416-464.

Mukherjee, M., L. Shu, and D. Wang. 2018. "Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges". *IEEE Communications Surveys & Tutorials* 20(3): 1826-1857.

Mustaffe, N., S. Brailsford, A. Djanatliev, T. Eldabi, M. Kunc, and A. Tolk. 2017. "Purpose and Benefits of Hybrid Simulation: Contributing to the Convergence of its Definition". In *Proceedings of the Winter Simulation Conference*, ed. by W. K. V. Chan, A. D'Ambrogio, G. Zacharewicz, N. Mustafee, G. Wainer, and E. Page, 1631–1645, Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc..

Mustafee, N. and J. H. Powell. 2018. "From Hybrid Simulation to Hybrid Systems Modelling". In *Proceedings of the 2018 Winter Simulation Conference*, ed. by M. Rabe, A .A. Juan, N. Mustafee, A. Skoogh, S. Jain, and B. Johansson, 1430-1439, Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Nagothu, D., R. Xu, S. Y. Nikouei, and Y. Chen. 2018. "A Microservice-enabled Architecture for Smart Surveillance Using Blockchain Technology". arXiv preprint arXiv:1807.07487.

Nakamoto, S. 2008. "Bitcoin: A Peer-to-peer Electronic Cash System". October 31.

Neal, S., R. Fujimoto, and M. Hunter. 2016. "Energy Consumption of Data Driven Traffic Simulations". In *Proc. of the 2016IEEE Winter Simulation Conference*, edited by T. M. K. Roeder, P. I. Frazier, R. Szechtman, E. Zhou, T. Huschka, and S. E. Chick, 1119-1130.Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Nikouei, S. Y., Y. Chen, A. Aved, and E. Blasch. 2018a. "Eiqis: Toward an Event-oriented Indexable and Queryable Intelligent Surveillance System," arXiv preprint arXiv:1807.11329.

Nikouei, S. Y., Y. Chen, S. Song, R. Xu, B-Y. Choi, and T. R. Faughnan. 2018b. "Intelligent Surveillance as an Edge Network Service: from Harr-cascade, Svm to a Lightweight CNN". arXiv preprint arXiv:1805.00331.

Nikouei, S. Y., Y. Chen, S. Song, and T. R. Faughnan. 2018c. "Kerman: A Hybrid Lightweight Tracking Algorithm to Enable Smart Surveillance as an Edge Service". arXiv preprint arXiv:1808.02134.

Nikouei, S. Y., R. Xu, D. Naogothu, Y. Chen, A. Aved, and E. Blasch. 2018d. "Real-time Index Authentication for Event-oriented Surveillance Video Query using Blockchain". arXiv preprint arXiv:1807.06179.

Nikouei, S. Y., Y. Chen, S. Song, R. Xu, B-Y. Choi, and T. R. Faughnan. 2018e. "Real-Time Human Detection as an Edge Service Enabled by a Lightweight CNN". In *Proc. Of the 2018IEEE International Conference on Edge Computing*, July 2nd-7th, San Francisco, CA, USA, 125-129.

Nikouei, S. Y., R. Xu, Y. Chen, A. Aved, and E. Blasch. 2019. "Decentralized Smart Surveillance through Microservices Platform". *Proc. SPIE 11017*, May 28th, Baltimore, MD, USA, 1-16.

Onggo, B. S., N. Mustafee, A. Smart, A. A. Juan, and O. Molloy. 2018. "Symbiotic Simulation System: Hybrid Systems Model meets Big Data Analytics". In *Proc. of the 2018 Winter Simulation Conference*, ed. by M. Rabe, A. A. Juan, N. Mustafee, A. Skoogh, S. Jain, and B. Johansson, 1358-1369, Institute of Electrical and Electronics Engineers, Inc..

Piciarelli, C., L. Esterle, A. Khan, B. Rinner, and G. L. Foresti. 2016. "Dynamic Reconfiguration in Camera Networks: a Short Survey". *IEEE Transactions on Circuits and Systems for Video Technology* 26(5): 965–977.

Ribeiro, M., A. E. Lazzaretti, and H. S. Lopes. 2018. "A Study of Deep Convolutional Auto-encoders for Anomaly Detection in Videos". *Pattern Recognition Letters* 105: 13-22.

Shekar, S. 2016. "Dynamic Data Driven Cloud Systems for Cloud-Hosted CPS". In *Proc. of the 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW*), Apr. 4th-8th, Berlin, Germany, 195-197.

Snidaro, L., J. Garcia Herrero, J. Llinas, and E. Blasch (Eds.). 2016. *Context-Enhanced Information Fusion*: *Boosting Real-World Performance with Domain Knowledge*, Heidelberg, Germany:Springer.

Sultana, T., and K. A. Wahid. 2019. “Choice of Application Layer Protocols for Next Generation Video Surveillance using Internet of Video Things”. *IEEE Access*, 7: 4607-41624, DOI: 10.1109/ACCESS.2019.2907525.

Szabo, N. 1997. “Formalizing and Securing Relationships on Public Networks”. *First Monday* 2(9).

Van Eeden, W. D., J. P. de Villiers, R. J. Berndt, W. A. J. Nel, and E. Blasch. 2018. “Micro-Doppler Radar Classification of Humans and Animals in an Operational Environment”. *Expert Systems With Applications* 102: 1-11.

Wei, M., E. Blasch, G. Chen, J. B Cruz Jr, L. Haynes, M. Kruger, and I. Sityar. 2007. “Game Theoretic Behavior Features Change Prediction in Hostile Environments”. *Proc SPIE 6567*, May 7th, Orlando, FL, USA, 1-9.

Wu, J. 2015. “Mobility-enhanced Public Safety Surveillance System using 3DCameras and High Speed Broadband Networks”. GENI NICE Evening Demos.

Wu, R., B. Liu, Y. Chen, E. Blasch, H. Ling, and G. Chen. 2015. “Pseudo-real-time Wide Area Motion Imagery (WAMI) Processing for Dynamic Feature Detection”. *International Conf. on Information Fusion*, July 6th-9th, Washington, DC, USA, 1962–1969.

Wu, R.,B. Liu, Y. Chen, E. Blasch, H. Ling, and G. Chen. 2016. “A Container-based Elastic Cloud Architecture for Pseudo Real-time Exploitation of Wide Area Motion Imagery (WAMI) Stream”. *Journal of Signal Processing Systems* 88(2): 219-231.

Wu, R., B. Liu, Y. Chen, E. Blasch, H. Ling, and G. Chen. 2017. “A Container-based Elastic Cloud Architecture for Pseudo Realtime Exploitation of Wide Area Motion Imagery (WAMI) Stream”. *Journal of Signal Processing Systems* 88(2): 219–231.

Xu, R., S. Chen, L. Yang, Y. Chen, and G. Chen. 2019a. "Decentralized Autonomous Imaging Data Processing using Blockchain.” *Proc. SPIE 10871*, Feb. 27th, San Francisco, CA, USA, 1-16.

Xu, R., S. Y. Nikouei, Y. Chen, S. Song, A. Polunchenko, C. Deng, and T. Faughnan. 2018d. “Real-time Human Object Tracking for Smart Surveillance at the Edge”. *The 2018 IEEE International Conference on Communications, Selected Areas in Communications Symposium Smart Cities Track* (ICC SmartCities 2018), May 20 h-24th, Kansas City, MO, USA, 2018.

Xu, R., Y. Chen, E. Blasch, and G. Chen. 2018a. “BlendCAC: A Blockchain-enabled Decentralized Capability-based Access Control for IoTs”. *IEEE International Conference on Blockchain (Blockchain-2018),*August 1st-3rd, Halifax, Canada, 1–8.

Xu, R., Y. Chen, E. Blasch, and G. Chen. 2018b. “BlendCAC: A Smart Contract enabled Decentralized Capability-based Access Control Mechanism for the IoT”. *Computers* 7(3): 39.

Xu, R., Y. Chen, E. Blasch, and G. Chen. 2019b. “Exploration of Blockchain-enabled Decentralized Capability-based Access Control Strategy for Space Situation Awareness”. *Optical Engineering* 58(4): 041609.

Xu, R., X. Lin, Q. Dong, and Y. Chen. 2018c. “Constructing Trustworthy and Safe Communities on a Blockchain-enabled Social Credits System”. *EAI International Conf. on Mobile and Ubiquitous Systems: Computing, Networking and Services*, November 5th-7th, New York, NY, USA, 449–453.

Zheng, Y., E. Blasch, and Z. Liu. 2018. *Multispectral Image Fusion and Colorization.* SPIE Press. Bellingham, WA:

Zheng, Y., W. Dong, and E. Blasch. 2012. “Qualitative and Quantitative Comparisons of Multispectral Night Vision Colorization Techniques”. *Optical Engineering* 51(8): 087004.

AUTHOR BIOGRAPHIES

ERIK BLASCH is a Program Officer at the Air Force Office of Scientific Research (AFOSR). He received his BS from MIT, six MS degrees, and PhD from Wright State University. He has compiled 800+ papers, 5 books, 27 patents, and 30 tutorials. He is a recipient of the Military Sensing Society Mignogna data fusion award, past president of the International Society of Information Fusion, AIAA Associate Fellow, SPIE Fellow, and IEEE Fellow. His email address is erik.blasch.1@us.af.mil.

RONGHUA XU is a PhD student of Electrical and Computer Engineering at the Binghamton University - State University of New York (SUNY). He earned his B.S. on Mechanical Engineering from Nanjing University of Science & Technology, China in 2007, and received his M.S. degree on Mechanical and Electrical Engineering from Nanjing University of Aeronautics & Astronautics in 2010. His research interest lies in Machine Learning; Blockchain, Algorithm Design; Cloud/Fog/Edge Computing Paradigm.. His email address is rxu22g@binghamton.edu.

SAYED YAHYA NIKOUEI is a Ph.D. student at the Binghamton University and his research focuses on Machine Learning, pattern recognition, specifically for the lightweight designs in the Edge-Fog-Cloud Computing paradigm and the applications in Smart Cities such as the smart surveillance system and public safety. He earned his BS in 2014 and MS in 2016 both in Electrical Engineering specializing in random hierarchy algorithms to optimize Inverter performance. His email address is snikoue1@binghamton.edu.

YU CHEN is an Associate Professor at the Binghamton University-SUNY. He received the Ph.D. in Electrical Engineering from the University of Southern California(USC) in 2006. His research interest lies in Trust, Security and Privacy in Computer Networks, focusing on Edge-Fog-Cloud Computing, Internet of Things (IoT), and their applications in smart and connected environments. His publications include over 150 papers in scholarly journals, conference proceedings, and books. His email address is ychen@binghamton.edu.