The Center of Excellence for Communication Systems Technology Research

CECSTR CURRENT RESEARCH PROJECT ACTVITIES

Research Topic: Development of a Blockchain-Based Edge Computing Security Broadband Research for IoT in the Era of 5G and Millimeter Wave Communication Systems

Principal Investigator: Prof. Cajetan M. Akujuobi, Ph.D., MBA, P.E., F.I.A.A.M.
Phone: 936-261-9991. **Email:** cmakujuobi@pvamu.edu

Doctoral Graduate Assistant: Faith Nwokoma

Synopsis of the Research Project

The cloud, particularly, the distributed cloud and software-defined networking and network function virtualization have become popular in many broadband and blockchain-based edge computing security networks in this era of 5G and millimeter wave communication systems. As the industry explores more flexible, automated network solutions, this part of the evolution toward 5G capabilities is already underway. However, the research questions remain on the best network architectures for different applications. Ultra-low-latency applications such as autonomous driving may require highly distributed networks simply due to the laws of physics, while applications that can tolerate higher latency could be served from fewer central locations.

Blockchain has become a major technology that can now be used in the management of decentralized systems. It has gained momentum in many application areas such as healthcare systems, precision agriculture and smart grid. The Internet of Things (IoT) has also grown to a magnitude where we have billions of IoT devices connected online. IoT is increasingly being adopted in many application scenarios, powering smart cities, smart grid, smart manufacturing, smart home, and smart agriculture where it enables flexible information and resource sharing. Blockchain operates as a decentralized ledger that can be used to verify and store records of transactions and has been shown to perform better than its counterpart systems that are based on centralized digital ledgers.

However, utilizing this core technology in resource-constrained mobile devices is very much limited because of high demands of resources and poor scalability with frequent-intensive transactions. This becomes absolutely necessary to look at edge computing

which can be integrated to facilitate mobile 5G broadband devices in offloading their mining tasks to cloud resources in the era of millimeter communication systems. The main stumbling blocks still remaining in this integration process is the realization of the security aspects and the decentralized management in edge computing. This integration process has the capability of ensuring key reliable access, distributed computation and untampered storage for scalable secure transactions. Lots of studies have been conducted in the exploration of suitable architectural requirements, and some of the researchers have applied the integration to deploy some of the specific applications.

Despite the ongoing efforts for a suitable platform for block chain deployment in IoT applications; anonymity, adaptability and data integrity are crucial issues that are yet to be solved to ensure safe storage of data. Since only pseudonyms are guaranteed in block chain, and integrity relies only on massive numbers of honest miners and proof-of-Work's (PoW's) complexity (which also affects the scalability); investigation for appropriate technologies to provide stronger anonymity than just pseudonymity and achieve adaptable data integrity must be investigated further to achieve an edge-based practical, secure decentralized data storage which this study will do.

Edge computing also faces cyber-attacks. The cyber-attack, such as the denial of attack, man-in the-middle attack at the edge computing will cripple the IoT applications. Although the IT-based firewall protection can protect some of the cyber-attacks, it is not a bullet-proof solution. A zero-day attack is difficult to detect in the IoT environment. Artificial intelligence (AI) can be implemented to detect a zero day attack, but AI requires a good training dataset for IoT applications. There are not many suitable IoT datasets for this purpose. This study will also focus both on the block chain to achieve an Internet of Things (IoT) design supported by edge computing to acquire security and scalability levels needed for integration and proper resource management, and network intrusion detection (NID) for edge computing system by developing a new IoT dataset and artificial intelligence-based NID system.

Research Expectations

This research is expected to yield the following results:

- Development of a blockchain-based edge computing security broadband network for IoT suitable for 5G and millimeter wave communication systems.
- Suitable architectural network requirements applicable to the integration and deployment to some specific 5G and millimeter wave communication systems applications.
- Development of a suitable platform for blockchain deployment in IoT applications ensuring anonymity, adaptability and data integrity for safe storage of data.
- Investigation for appropriate technologies to provide stronger anonymity than just pseudonymity capable of achieving adaptable data integrity that must further achieve an edge-based practical, secure decentralized data storage.

- Implementation of an artificial intelligence (AI) that can detect a zero day attack with good training dataset for IoT applications.
- Finally, developing a test bed capable on focusing both on the block chain to achieve an Internet of Things (IoT) design supported by edge computing to acquire security and scalability levels needed for integration and proper resource management, and network intrusion detection (NID) for edge computing system by developing a new IoT dataset and artificial intelligence-based NID system.