FIU Cybersecurity
FLORIDA INTERNATIONAL UNIVERSITY

Research Statement

Kemal Akkaya
Department of Electrical and Computer Engineering
Florida International University

1 Introduction

Motivated with the proliferation of smart, low-cost and small devices, there is a growing trend towards the development of smart buildings, cities, and infrastructures in order to make our lives more efficient, cleaner, safer and less costly than before. Examples of these devices include smart sensors, meters, phones, tablets, cameras, drones, wearable technologies (e.g., glasses, watches) and cars that are currently ubiquitous. These smart devices have typically computation, communication, sensing, and storage capabilities and have been the focus of a great deal of research in the last two decades. Such research activities range from the hardware/software characteristics of these individual devices to their deployment challenges in the development of smart infrastructures that involve wireless communications at various levels. This led to the conceptualization of these ideas under the names Internet-of-Things (IoT) and Cyber-physical Systems (CPS), latter adding the capability of interaction with the physical systems.

In addition to challenges that are related to networking/communication aspects, IoT and CPS are also vulnerable to various networking and software attacks that may include malware, unauthorized device/network access, jamming, impersonation, privacy breaches, data modification, etc. My research has been exploring the communication security and privacy aspects of CPS and IoT. My main work revolved around security and privacy-aware protocol design that can utilize tools from applied cryptography, game theory, graph-theory and social sciences. To this end, I founded Advanced Wireless and Security (ADWISE) Lab in 2008. At ADWISE Lab, we have published extensively at top venues in the past [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11]. While my lab still continues pursuing research around these themes, my recent research started to be influenced greatly with the ongoing transformations in broader cybersecurity domain. Specifically, the domination of the cybersecurity technologies in every application and field brought new challenges due to their practical deployment and interaction with users/apps. I observed that these challenges can be categorized under engineering, management and user aspects. Let me briefly explain each of these items.

Security engineering refers to development of secure systems by efficiently bringing different tools together geared for a specific application. For instance, depending on the application restrictions such as bandwidth, delay, costs, etc., we design protocols for authentication, key agreement and privacy to meet these objectives. This may involve utilizing tools from applied cryptography, game theory or blockchains. Sample research projects are given in Section 2.1.

Security management is an emerging concept which deals with the maintenance of the existing secure systems. One of the major issues under this item is to manage security keys and certificates. Another issue is to update intrusion detection/prevention system models with the ever changing attack environments. There are many other aspects which may include dealing with third parties, cloud and internal users. Please refer to sample research projects in Section 2.2.

User aspects of security is a very broad area and brings many critical issues into perspectives in terms of privacy, usability and cyber crime. The top concern of user privacy already led to a

new domain referred to as *privacy-enhancing technologies* (PETS). We explore one of these PETS, namely secure multi-party computation (MPC) to be efficiently run on cloud environments. Cyber crime represents another user aspect of cybersecurity since prosecution of these crimes depend on novel *digital forensics* frameworks which may be using various machine/deep learning techniques. Our recent research investigated some novel solutions to be used within cyber crimes research. Some sample research projects are listed in Section 2.3. Next, I elaborate on the ongoing projects at Advanced Wireless and Security (ADWISE) Lab led by me at FIU.

2 Current Projects

I have several ongoing projects as part of my research. While some of the projects have already yielded a number of publications and patents, there are still many future challenges to address. For the rest of the projects, the research is still active for design, development and publications.

2.1 Security Engineering

5G OpenRAN Fronthaul Security: The Open-RAN Fronthaul transports very sensitive data between Radio Units and Distributed Units over Ethernet which is part of 5G Core. Control, User, Synchronization, and Management packets are exposed to different types of threats due to the lack of implemented security standards. There are four pillars of security that should be satisfied by any security standard chosen to protect the Open-RAN Fronthaul; these are Confidentiality, Integrity, Authenticity, and Availability.

In this project, we explore the usage of Fronthaul transport protocols such as the Common Public Radio Interface (CPRI). Typically, 5G communications were only secured over the air, between the user equipment and the base station. Between the base stations and the core network no security was implemented. This project seeks to explore options for securing transport over this fronthaul (i.e., base station to core network) while keeping the additional overhead introduced to a minimum, as well as to explore options/behavior for securing such in a post-quantum environment.

We are exploring protocols such as Transport Layer Security (TLS) and IEEE 802.1AE (MACSEC), focusing on characteristics such as speed, efficiency, and delay as some 5G services have strict timing synchronization requirements. We mainly focus on MACSEC specifically because of its reduced overhead compared to the previous two. It is like IPSec, but it works at the data-link layer and is more lightweight.

Enabling Third Layer Bitcoin Applications using Lightning Network: In recent years, many cryptocurrencies started being used in various daily-life applications. In particular, Bitcoin has been gaining tremendous popularity which was fueled by the revolutionary blockchain concept. Its market cap is now above 50% among all cryptocurrencies. Nevertheless, Bitcoin's transaction fees are still high and payment verification times are generally more than 10 minutes, which makes it unfeasible for real-time transactions. To address this issue, different schemes have been proposed. Among these, the most widely adopted one is the Lightning Network (LN). The idea is to utilize smart contracts and avoid writing every transaction to the blockchain. Instead, the transactions are recorded off-chain until the accounts are reconciled. Specifically, once a channel is created between two peers, many off-chain transactions can be performed in both directions as long as there are enough funds. When many nodes come together, the off-chain payment channels turn into a network, referred to as a payment channel network (PCN), such as LN. As of today, LN

grew to more than 17K users in three years, making it a popular environment for instant Bitcoin transactions.

The emergence of LN opened new doors to many potential novel applications that can utilize its infrastructure. Indeed, LN's underlying network offers a perfectly covert communication medium to enable security and privacy by default. This creates opportunities for the sake of good and bad. This project aims to demonstrate both types of applications that can rely on or exploit LN, which are referred to as third-layer applications assuming that Bitcoin is the first and LN is the second layer. We tackled the challenges of building third-layer LN applications in two practical use cases.

The first practical application we target is the utilization of LN for enabling micro-payments (i.e., paying with your smartwatch or vehicle) for resource-constrained IoT devices without dealing with credit card payments. For this purpose, we introduce two protocols that enable IoT devices with limited resources to be able to use LN without installing LN or Bitcoin software. The first approach is based on a designated gateway node to act on behalf of an IoT device to open & close LN channels and transact with other users. To guarantee trustless operations, we introduce 3-of-3 multisignature LN channels which secure the IoT device's funds even when the gateway is malicious [12]. More specifically, the gateway needs the IoT device's cryptographic signature for every LN operation, when not provided, operations such as channel opening closing or payment sending cannot be completed. To incentivize the gateway, the IoT device pays fees to the gateway for every transaction it performs. The second protocol aims to improve this protocol by using threshold cryptography instead of 3-of-3 multisig [13]. By using threshold cryptography, the channel structure of LN does not need to be modified. Another advantage of the threshold method is the smaller transaction size which reduces the transaction fees paid by the IoT device and the gateway. We extended the threshold work by analyzing the security of the protocol using game theory and extended the implementation with Bluetooth experiments.

While LN can enable useful applications such as IoT micro-payments, it can also be exploited for malicious purposes. For this use case, we show how LN can be used to control a botnet through highly anonymous covert communication. We introduce LNBot which is a covert hybrid botnet running on top of LN by utilizing various anonymity features of LN to operate [8]. By encoding messages using LN payments, we show that it is very hard to shut down LNBot because of the strong anonymity features of LN such as its onion-routed payments. We extended this work such that the botnet can form itself distributively removing the need for any manual intervention from the botmaster.

Our current work is about enabling offline LN payments in a mobile mesh network setting where the nodes do not have Internet connectivity and can move around. We already have proof of concept implementation of the idea using both Bluetooth and WiFi for the communication protocol. We explore channel assignment strategies to best fit the mobility model of the users.

Optimal Incentive Mechanism for Fair and Equitable Rewards in PoS Blockchains: Blockchain technology offers many powerful use cases while promising the establishment of distributed autonomous organizations (DAOs) that may transform our current understanding of client-server interactions in cyberspace. They employ distributed consensus mechanisms that have been subject to a lot of research in recent years. While most of such research focused on the security and performance of consensus protocols, less attention has been given to their incentive mechanisms which relate to a critical feature of blockchains. Unfortunately, while blockchains are advocating decentralized operations, they are not egalitarian due to existing incentive mechanisms. Current consensus protocols inadvertently incentivize the centralization of mining power and inequitable

participation.

This project explores and evaluates alternative incentive mechanisms for more decentralized and equitable participation. Borrowing from taxation literature in Economics, we propose three alternatives in which the reward scheme is more partial to low stakeholders either by providing transfers from rewards or increasing the rate of rewards for the 'poor'. Through simulation, we test how existing PoS-based incentive mechanisms and our proposed alternatives affect the accumulation of wealth in the long run. We evaluate these mechanisms under different settings including various levels of reward rate, number of nodes, and initial wealth distributions.

The offered mechanisms could create adverse incentives for high stakeholders to hold multiple low-stake nodes to increase benefits from rewards. Therefore, we also propose a blockchain mechanism where selection to block generation relies on reputation-like scores as well as owned stakes. We also plan to employ Game theoretic models to explore the optimum reward schedule for low- and high-stakeholders. This project is funded in part by US National Science Foundation and already led to a publication [14].

2.2 Security Management

Development of an Open-source SDN-based Testbed for 5G SA: Since the introduction of the first-generation mobile network in the 1980s, mobile wireless communication requirements have been growing significantly over the past decade, from analog phone calls to real-world applications such as autonomous vehicles, remote surgeries, and advanced robotics. These real-world applications depend on three fundamental building blocks required for 5G networks: Enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communications (URLLC), and Massive Machine Type Communications (mMTC) that will allow more devices to connect at once, faster data rates, and lower latency. In order to deliver these requirements, it is necessary to apply different technologies to provide customization, flexibility, and management in the 5G network, such as Software-Defined Networks (SDN) and Network Function Virtualization (NFV). SDN and NFV will help to manage the resources better, enable scalability, manage the network from a centralized perspective, and restore system functionality after an attack. Also, it is possible to apply different mitigation services against anomalies in the network using machine learning.

This project builds a 5G SDN testbed using open-source tools such as Openstack and Onos for SDN capabilities, Open5Gs for the core network, and srsRAN for the gNB simulation. This testbed can be used for various research purposes including network & security management, testing of security protocols, and performance analysis of 5G intrusion detection services. This project is funded by US National Science Foundation and NSA.

Efficient Key Management for Low-bandwidth Publish-Subscribe Networks: The underlying legacy communication infrastructures, which may have severely constrained bandwidth, are under a lot of strain as a result of adding new smart devices and increased data collection for better control decisions in the Smart Grid infrastructure. Therefore, publish-subscribe architectures are becoming common, which not only enables flexible communication options but also takes advantage of the multicast/broadcast abilities to minimize the amount of data messages transmitted.

To enable secure multicast/broadcast data exchange, there must be underlying mechanisms to generate keys in any of these scenarios. A group key is employed for protecting the authenticity, integrity, and confidentiality of broadcast messages. Although the generation of session keys for

unicast communications has been the subject of extensive research, this does not entirely apply to group communications (i.e., key generation, distribution, and renewal) in Smart Grid environments. In addition, there needs to be efficient mechanisms for any type of key generation to minimize the disruption to data traffic when keys are being updated frequently.

This project focuses on achieving an efficient key management schemes to secure both unicast and broadcast communications in publish-subscribe (i.e., OPC UA) based Smart Grid applications. For instance, one component of the project explores a secure key management scheme that integrates the dynamic key-generation with Shamir's secret sharing to achieve efficient group key management [15]. The other component investigates more efficient broadcast for the widely used DDS protocol. This work is supported in part by USAID Organization.

2.3 User Aspects of Security

Efficient and Practical Secure Multiparty Computation in Zero-trusted Environments: Privacy Enhancement Technologies (PET) have gained attention in domains where privacy is essential, such as health analysis, financial analysis, machine learning, big data, etc. Homomorphic Encryption (HE) and secure multi-party computation (MPC) are two major approaches. The advances in research on these technologies were mostly at the theoretical level for many years. However, the focus shifted to their practical deployments and performance improvements during the last decade. In particular, research on the MPC side has been accelerated as it is faster than fully homomorphic encryption (FHE). MPC consists of several mutually distrusted parties, which hold a share or secret of each private value, and jointly evaluate a function without leaking any information other than the respective output.

While there have been notable advances in improving MPC performance, there are still several challenges ahead, not only related to further efficiency improvements but also in other aspects that are critical for their broad adoption, such as robustness, correctness verification, and management, including initial MPC setup and maintenance. For instance, there is a lack of solutions that handle real-world events such as participants joining or leaving the system, the coordination among clients and MPC service providers, handling failures, and more.

This project focuses on enhancing the MPC efficiency from the networking and management perspectives and proposing a protocol that automates the MPC system setup and management without degrading the efficiency. Some features include use of blockchain communication channel, participants registration (e.g., MPC server, input clients), authentication among participants, orchestration of MPC tasks, correctness verification, output delivery, and resumption of computation in case of node failures. This project is supported in part by the US National Science Foundation and the US Air Force and already led to two publications [16][17].

Robust and Privacy-preserving Federated Learning through Secure Multiparty Computation: The interest in Privacy Preserving technologies has increased in recent years, and it is now making its way to private and public sector applications that use private data. Similarly, the increased usage of Machine Learning (ML) in many applications requires big datasets that are not easily accessible for individual companies or handled by different departments in those organizations. A good solution to this challenge of training on distributed datasets is Federated Learning (FL). It allows organizations or governments to collaborate in training ML models without sending raw data. This helps train more robust ML models from localized data but does not prevent attacks on the models generated from such data.

While there are several privacy-preserving technologies used to protect the models like Multi-party Computation (MPC), Fully Homomorphic Encryption (FHE), and Differential Privacy (DP), we propose using MPC to enable a comprehensive service for FL. The reason is that MPC offers higher security guarantees, while not compromising the accuracy of the models or using an excessive amount of hardware resources. Additionally, we can run the aggregation phase of FL in a dishonest majority setting (i.e., the majority of the parties are not trusted), while keeping our model distributed among the participating MPC parties. While the model is distributed, the MPC protocol allows us to perform a range of complex operations on the model without revealing any details about it.

We propose a system model that takes advantage of the distributed nature of MPC to help train on highly sensitive data such as government-collected data or user-collected data (e.g., health records). Our aim with this system is to conduct training on dishonest majority networks while utilizing the least amount of resources possible.

This work is supported in part by US National Science Foundation and AFRL.

Multimedia Forensics - Source Camera Identification: Multimedia forensics gained attention due to the wide usage of various recording sources and IoT devices. At the same time, the rapid technological developments caused the escalation of forgeries and data tampering of media files. Therefore, the integrity and origin of video and image data coming from cameras which may be on drones or smartphones became one of the key challenges in digital forensics. The lenses' defects introduced during the manufacturing process produce unique patterns, namely fingerprints, that can be used for source camera identification.

For a long time, the photo response non-uniformity (PRNU) detection techniques were used to generate a unique camera fingerprint and then use it as a ground truth. While PRNU is still widely applied for image source camera detection, it has proven less effective for videos. Deep Learning (DL) techniques, specifically Convolutional Neural Networks (CNNs) have been applied. Unlike PRNUs, CNNs allow to effectively extract camera-specific features from a given set of videos, while reducing the impact of compression effects.

This project focuses on enhancing the accuracy of CNN applications for video source camera identification. Moreover, we analyze the network's resistance against the source camera falsification attacks, to further strengthen the proposed framework. To improve the network, we conduct an interpretability analysis of the designed video source identification network. As a result, we identify how CNN "makes its decisions" and make it more robust and lightweight.

This work is supported in part by grants from the US National Science Foundation and the Army Research Office. The project already led to two publications [18, 19].

Cryptocurrency Artifact Detection on Android Devices: When the user performs transactions from the crypto wallet or browses the Internet for crypto then it generates artifacts such as mnemonics phrases, transactions history, images related to crypto, web cookies, and so on. These artifacts are very important for investigators, so the detection and extraction of the artifacts is needed. This project aims to build a triage tool for automatic extraction of the artifacts from Android phones to present to the investigator. Mainly this tool focuses on three major components – Crypto wallet application, Images, and Web history.

It integrates contemporary approaches from machine learning, natural language processing and pattern recognition to be able to detect any artifact that may potentially come from the recently launched crypto wallet apps. For the images, the tool automatically detects and extracts the

cryptocurrency information. We analyze all the web browsers from the phone and search for the relevant artifacts as well. These findings which can come from apps, images or browsing history are displayed separately with an option to check further details. We also explore the analysis of SMS, and different language support for the tool. This project is funded by Drug Enforcement Administration (DEA) and US National Science Foundation.

3 Future Research

My future research will still build on my existing research agenda but I would like to explore a number of promising directions. These areas are listed below.

3.1 Distributed Autonomous Organizations - Web3.0

Current applications and communities in cyberspace are designed based on the legacy client-server model which eventually led to the centralization of services by a specific set of entities (e.g., Amazon for cloud services, Google for web search, Facebook for social media, etc.). As these entities have grown, the centralization has also grown, raising criticism in terms of power, social equity, user privacy, and security. With the emergence of blockchain, there is a growing interest to initiate a paradigm shift in the way online services are managed. As such, a lot of new applications/communities referred to as 'decentralized autonomous organizations' (DAOs) have emerged recently that rely on peer-to-peer (P2P) blockchain technologies and have the potential to address the concerns with centralized architectures in terms of equal participation, user privacy, and economic mobility. However, the widespread adoption of these DAOs (aka Web3.0) that will enable the same service quality as the centralized model in terms of scalability, reliability, availability, timeliness, affordability, interoperability, and usability is still far from reality due to several theoretical and practical challenges. We plan to explore a convergent approach to these multifaceted challenges to help revolutionize the way we manage the de facto cyberspace by realizing and proliferating the DAOs in all relevant domains. This will lay out a comprehensive rigorous research agenda by merging the benefits of the P2P and client-server models while paying attention to scalability, equity, performance, security and privacy.

3.2 Post-quantum Security Management for Next Generation Systems

With upcoming promise around 5G/6G systems as well as the potential of satellite networks to challenge the existing paradigms, there are also a lot of efforts in integrating millions of Internet of Things (IoT) devices through a virtualized, slice and cloud-based architecture. Referred to collectively as Next Generation Networks (NextG), this revolution will also expand the attack surface for cyber threats arising from both classical as well as quantum computers due to softwarization, open interfaces and unattended IoT devices. As the progress in building quantum computers is becoming more realistic, it is prudent to adapt end-to-end quantum-resistant cryptography protocols into the NextG systems as we design and deploy them.

Realizing this challenge, this research will integrate concepts from quantum-safe device level security, wireless networking, security management and network evaluation in ways that have not been studied before. Specific problem areas being addressed include (i) investigation of quantum-safe cryptography algorithms for IoT devices deployed NextG systems, (ii) efficient quantum-safe

certificate management in NextG systems, and (iii) end-to-end deployment and evaluations of quantum-safe cryptography in NextG systems.

3.3 Cyber Crime

The prolific use of digital documentation since the 2000s, transformation of business and government services through online tools, and the transitioning to mobile phone based systems introduced many new challenges for data storage, provenance and data authenticity within the forensic community. Majority of the crimes now include digital tools and technology which require a deeper look in to cyber forensics domain. However, at the same time as mentioned above, PETs are also heavily promoted which creates a tension between user privacy and safety. As such, it is not easy to have access to data and systems owned by third parties. This requires many new approaches to be investigated. First, the existing systems that are being developed should incorporate provenance capability by design. This may include machine learning models that produce certain outputs without providing any justification. The owner of applications should be able to trace any activity whether it is run on cloud environments or through a machine learning model. For instance, NextG systems should have mechanisms that may be based on blockchain technologies to store the needed information. The second item in this research is the ability to protect user privacy when conducting digital forensics investigations. While checking for specific information, the other data can also be exposed to other parties which poses a privacy issue. Therefore, privacy-preserving analysis techniques should be explored. A final item under this type of research is to research theoretical aspects of forensics and formalize this process to offer a more scientifically sound evidence gathering.

3.4 Privacy/Security and Policy

PETS have already been a major issue and supported initiative by the White House. This means that privacy will be a top debated issue within the policy circles. Indeed, there were major efforts in previous years such as European Privacy Law (GPDR) and another bills on IoT privacy/security is also being discussed in EU. The US also considers several new bills at the state or federal level. This means from the policy perspective there needs to be continuous efforts to explore the optimal policy considerations. This includes setting standards for the governments and industries by considering users' needs. This interdisciplinary research agenda will involve experts from the public policy and law domains to offer engineering solutions that will be easily integrated with existing standards. For instance, if government entities would like to follow a zero-trust framework for their networks, then solutions enforcing authentication and authorization should consider this framework within their protocols (e.g., apply continuous authentication).

References

[1] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 50–57, 2018.

[2] A. Acar, W. Liu, R. Beyah, K. Akkaya, and A. S. Uluagac, "A privacy-preserving multifactor authentication system," *Security and Privacy*, vol. 2, no. 5, p. e88, 2019.

[3] A. Aydeger, N. Saputro, and K. Akkaya, "A moving target defense and network forensics framework for isp networks using sdn and nfv," *Future Generation Computer Systems*, vol. 94, pp. 496–509, 2019.

[4] A. Acar, H. Aksu, S. Uluagac, and K. Akkaya, "A usable and robust continuous authentication framework using wearables," *IEEE Transactions on Mobile Computing*, to appear.

[5] E. Bulut, M. C. Kisacikoglu, and K. Akkaya, "Spatio-temporal non-intrusive direct v2v charge sharing coordination," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 10, pp. 9385–9398, 2019.

[6] M. Cebe and K. Akkaya, "A replay attack-resistant 0-rtt key management scheme for low-bandwidth smart grid communications," in *Proceedings of the IEEE Global Communications Confernce (GLOBECOM'19), Hawaii, US*, Dec. 2019.

[7] D. Gabay, K. Akkaya, and M. Cebe, "Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5760–5772, 2020.

[8] A. Kurt, E. Erdin, M. Cebe, K. Akkaya, and A. S. Uluagac, "LNBot: A covert hybrid botnet on bitcoin lightning network for fun and profit," in *European Symposium on Research in Computer Security*. Springer, 2020, pp. 734–755.

[9] S. Tonyali, K. Akkaya, N. Saputro, A. S. Uluagac, and M. Nojoumian, "Privacy-preserving protocols for secure and reliable data aggregation in iot-enabled smart metering systems," *Future Generation Computer Systems*, vol. 78, pp. 547–557, 2018.

[10] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, and A. Tuncer, "Uav-enabled intelligent transportation systems for the smart city: Applications and challenges," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 22–28, 2017.

[11] F. Yucel, K. Akkaya, and E. Bulut, "Efficient and privacy preserving supplier matching for electric vehicle charging," *Ad Hoc Networks*, vol. 90, p. 101730, 2019.

[12] A. Kurt, S. Mercan, E. Erdin, and K. Akkaya, "3-of-3 multisignature approach for enabling lightning network micro-payments on IoT devices," *ITU Journal on Future and Evolving Technologies*, vol. 2, no. 5, pp. 53–67, 2021. [Online]. Available: https://doi.org/10.52953/WZPC8083

[13] A. Kurt, S. Mercan, O. Shlomovits, E. Erdin, and K. Akkaya, "Lngate: Powering iot with next generation lightning micro-payments using threshold cryptography," in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 117–128. [Online]. Available: https://doi.org/10.1145/3448300.3467833

[14] H. Sahin, K. Akkaya, and S. Ganapati, "Optimal incentive mechanism for fair and equitable rewards in pos blockchains," in *41st IEEE – International Performance Computing and Communications Conference (IPCCC)*, 2022.

[15] Y. Hanna, M. Cebe, S. Mercan, and K. Akkaya, "Efficient group-key management for low-bandwidth smart grid networks," in *2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2021, pp. 188–193.

[16] O. Bautista, K. Akkaya, and S. Homsi, "Outsourcing secure mpc to untrusted cloud environments with correctness verification," in *2021 IEEE 46th Conference on Local Computer Networks (LCN)*, 2021, pp. 178–184.

[17] O. G. Bautista and K. Akkaya, "Network-efficient pipelining-based secure multiparty computation for machine learning applications," in *2022 IEEE 47th Conference on Local Computer Networks (LCN)*, 2022, pp. 205–213.

[18] M. Veksler, R. Aygun, K. Akkaya, and S. Iyengar, "Video origin camera identification using ensemble cnns of positional patches," in *2022 IEEE 5th International Conference on Multimedia Information Processing and Retrieval (MIPR)*, 2022, pp. 41–46.

[19] E. Flor, R. Aygun, S. Mercan, and K. Akkaya, "Prnu-based source camera identification for multimedia forensics," in *2021 IEEE 22nd International Conference on Information Reuse and Integration for Data Science (IRI)*, 2021, pp. 168–175.