IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 4, 2022, accepted April 17, 2022, date of publication April 21, 2022, date of current version May 4, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3169141

Securing Digital Ledger Technologies-Enabled IoT Devices: Taxonomy, Challenges, and Solutions

ANASTASIOS N. BIKOS[1] AND SATHISH A. P. KUMAR[2], (Senior Member, IEEE)
[1]Department of Computer Engineering and Informatics, University of Patras, 26504 Patras, Greece
[2]Department of Electrical Engineering and Computer Science, Cleveland State University, Cleveland, OH 44145, USA

Corresponding author: Sathish A. P. Kumar (s.kumar13@csuohio.edu)

This work was supported by the Cleveland Foundation IoT Start-Up Grant under Project 200002018.

ABSTRACT With the faster maturity and stability of digitization, connectivity and edge technologies, the number of the Internet of Things (IoT) devices and sensors is flourishing fast in important junctions such as homes, hotels, hospitals, retail stores, manufacturing floors, railway stations, airports, oil wells, warehouses, etc. However, in this extremely connected world, the security implications for IoT devices are getting worse with the constant rise in malicious cyberattacks. The challenge is how to secure IoT sensors, services and data. The blockchain technology, a prominent distributed ledger technology (DLT), is being pronounced as the way forward for safeguarding IoT devices and data. The Directed Acyclic Graph (DAG)-based DLT has the inherent potential to realize the benefits of blockchain with better performance. IOTA is a DAG-based blockchain implementation for the IoT era. The Tangle, the IOTA's network immutably records the exchange of data and value. It ensures that the information is trustworthy and cannot be tampered with nor destroyed. In this work, we depict a thorough analysis of the existing security studies for IOTA. Then, we identify the gaps and the limitations of these security solution schemes, and finally, propose future security research recommendations that can potentially fill these gaps to secure DLT-enabled IoT devices.

INDEX TERMS Blockchain, decentralized, the IoT, IOTA, direct acyclic graph (DAG), Tangle, cybersecurity, privacy, confidentiality.

I. INTRODUCTION

Distributed Ledger Technologies (DLT) use a rather significantly modernized manner of consensus scheme amid non-trusted nodes over the non-centralized network. Numerous Internet of Things (IoT) devices would surely acquire merits of incorporating such a distributed consensus framework in a peer-to-peer manner. Thus, the necessity to leverage DLT with the IoT it is more prominent and beneficial than ever in the past. IOTA [16] is one of the (several) typical cryptocurrencies and digital ledger schemes that anticipates to become applicable for micro-payments and micro-transactions inside the machine-to-machine (M2M) economic ecosystem, not in the so distant future.

The Blockchain ledger [6] possesses essential attributes of decentralization, increased cybersecurity, portability, and increased-trust. This will inescapably allow DLT to settle the inherent practical considerations with IoT, such as its high infrastructural cost and resource dependability from their classical centralized perspective. Since the Blockchain communicates with *smart contracts* as part of its underlying functionality, it can afford paramount opportunities for the IoT world. To further clarify, a smart contract is typically an account whose states is entered, accessed, and written by any user terminal according to a set of preassigned functions. If this state refers to monetary values, a smart contract shall be able to circulate through financing activities, e.g., micro-payments and transactions among IoT appliances (*smart banking*). Another scenario is when a smart contract can simulate a central ''banking'' authority (validator) in a non-centralized intelligent power electricity application (e.g., smart grid metering), in these cases, the agreement (s) are updated and stored by the IoT devices themselves. Indeed, the application domain of such a primitive model is countless, including micro-transactions, smart cities, eHealthcare, remote medical operations, Telemedicine [5], smart electricity metering, intelligent homes, and even more critical Cyber-Physical-System Infrastructures (CPS). As we will discuss later, this fundamental model component drives the concept to enable the collaboration and enhancement of IoT through

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

the distributed ledger technologies. This also demands protocol described, architecture layer definitions, and of course, security and performing contracts handshaking between the devices and the validator through session modes [1], [2], and [7].

In such consensus scenarios, crucial considerations include (cyber)security, computational performance, and *Trust*. IoT systems include low resource constraint requirements, but besides, a most typical consensus algorithm fitted in IoT should include quite high *Turing* computational complexity in order to hinder forking or other malicious activities. There is, assuredly, a true mathematical challenge to define a proper consensus strategy (PoW/PoS) in the direction that IOTA would ideally attain this equilibrium trade-off between cybersecurity (from hardness) *as well as* resource-practicality, for such IoT integration. The classical Blockchain *cannot* meet these challenges for IoT incorporation needs.

To reduce the above shortcomings of Proof of Work (PoW) and/or Proof of Stake (PoS), a novel DAG consensus [16] permits any Peer to Peer (P2P) intermediate node to insert a new block into the decentralized ledger directly, given they process the parent transactions. This is a real gain for the recurrent micro-payments in the IoT systems. Despite the several advantages of IOTA (IoT/DAG integration), there exist still many security & privacy challenges. For instance, the immutability and irreversibility characteristics of the new ledger (Tangle) densely rely on cryptographic prototypes (e.g., hashing, permutations, etc.) that are generically probabilistic and are dependent on the reciprocal network conditions, because, as previously mentioned, this IOTA protocol interaction bears with inevitable security and privacy threats, such as Cyber attacks against the DAG ledger network, the consensus algorithms, the network access layer, or even worse the IoT devices themselves. Consequently, it is of vital significance to build confidentiality and integrity protection inside the previous model interaction [2]. Based on our research, we have provided an insightful comprehension of the security issues in the DAG consensus.

With even more ledger-based consensus mechanisms being suggested, as well as the growth of the IOTA open-source community, there is an emerging need to cover the full aspect of relevant investigated security & privacy issues. In this particular survey, we project a full comprehensive and illustrative review and analysis of the security implications inside the IOTA protocol deployment. Our unique contribution paradigm relies on existing literature to compare, depict and offer succinct sources for further evaluation [26]–[48], and [52]–[70].

To this end, this work makes the following contributions:

1) Builds a full attack classification and taxonomy for the IOTA security; defines most relevant security requirements or security classes for this new distributed ledger environment;
2) Investigates the related work on securing IoT within the scope of the distributed ledger enabled decentralized network (IOTA)
3) Identifies cybersecurity issues for the DLT-enabled Internet-of-Things applicability scenarios.
4) Recommends the security-related defense mitigation solutions from state-of-the-art literature studies to establish agile cyber security protection for the DLT-enabled IoT devices.

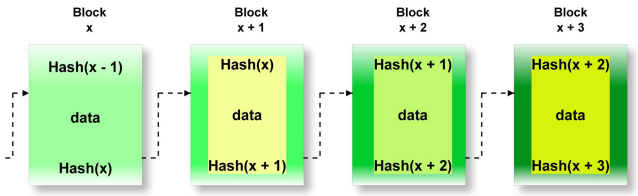


FIGURE 1. Blockchain concept: Blocks are linked via hash-pointer to rest blocks.

The rest of the manuscript is structured as follows. Section II defines basic concepts related to the distributed ledger technologies, important infrastructure considerations, as well as a brief introduction to the DAG concept. The Tangle consensus algorithm is also depicted in this Section, as well as the Internet-of-Things paradigm in terms of general layer-by-layer architecture. We utilize this layered approach to investigate the natural security deficiencies of IoT further and to justify why the IOTA-ledger integration seems promising to satisfy both security and performance challenges of traditional (non-decentralized) IoT. In Section III, we inspect the state-of-the-art cybersecurity attacks, threat models, exploitations, and vulnerabilities focusing on the new DAG concept as applied to IoT (IOTA). Based on those security challenges, in Section IV, we investigate which are the most studied IoTA security solutions and mitigations already found in the literature. In addition, we also suggest gaps and limitations from the IOTA perspective still unaddressed that deserve more attention. In Section V, we propose a security framework to protect IOTA. In Section VI, we explain future work based on challenges, existing solutions, and the gaps. Finally, Section VII concludes the research.

II. BACKGROUND: DLT FOR IoT DEVICES

Generic Block Chains gained significant fame after Nakamoto deployed the primary efficient crypto-currency structure based on blockchain technique, well-known as *Bitcoin* [6], inside which

the considerable challenge is to reassure the legitimacy of transactions (TXs) in the absence of a centralized ascendancy, or validator, mitigating, as much as possible, the ''double spending'' of ''virtualized'' money. This should, inevitably, not be assumed as inconsequential since Bitcoin/Blockchain nodes utilize a Peer-to-Peer (P2P) network(s) to make their own TXs public and, because of proliferation (propagation) lags, legal authorization nodes (validators) may concurrently admit two distinctive TXs that allocate the same funds but in a different order. They, therefore, must agree upon such consent (consensus) on which arrived primarily and is legitimate, together with which thereafter, as well as which is

not. Nakamoto's contribution was simply to order the TXs inside a chained sequence of timestamped and unique blocks (Blockchain), thus deploying a TXs transactional structure alongside a consensus or agreement means. Each block(s) includes a collection of Transactions, a timestamp, the hashing trace of the preceding validated block (for instance, its ''name''), together with the current date-time stamp (nonce), as depicted in Figure 1. A unique block is right, whether its factual data, cryptographically hashed with a double (recursive) SHA256 hashing function, derive a fingerprint that possesses a predefined set of trailing zeros. The node, actually, that gives birth to a block is furthermore permitted to aggregate a transaction to itself of a predefined level of Bitcoin that was ''mined'' inside this procedure as compensation for its processing job (e.g., mining the Blockchain). A blockchain abides, for instance, once a block is newly incremented, it can not be deleted, de-attached, or forged. Basically, every 'illegal' alteration of the last validated block would invalidate its hash name, which, as a result, illegitimate all the children's blocks. To trace a valid time stamp is computationally expensive, and due to this time complexity, the whole Blockchain architecture is named Proof of Work (PoW). Cryptominers tend to compete to retrieve the next successive block(s), which results in the notable *energy consumption problem of Bitcoin* [3].

Technically a PoW-based (ledger) blockchain is a data structure formation that deploys a dispersed and tamper-resistant shared ledger (SL) over a non-trusted computer network(s). Despite PoW not being the sole manner to satisfy the threshold on novel (block) chain blocks, there are even more energy agile means and techniques, especially if the network(s) is not always completely non-trusted [3].

A. AD-HOC AND MESH NETWORKS

Ad-Hoc and Mesh computer networks are typically recognized for their dynamic nature, a fundamental difference in scalability and complexity, as well as self-healing properties. They are commonly used to deploy multi-hop or multi-peer communications (MPC) among devices. In this paper, we argue that both these types of networks play a fundamental role in the infrastructure deployment of the PoW architecture.

1) AD HOC NETWORKS

A strictly ad-hoc network is characterized by its limited mobility, strict locality, and functionality, consisting of a few tens of portable devices. Ad-hoc networks can be technologically achievable to design/deploy, however, the mobile device operating system (OSs) can prevent someone from making such an operation. The reason is simply due to commercial policies, with no actual technical obstacles existing.

2) MESH NETWORKS

On the other hand, a mesh network could be seen as a more statically-built network deployment comprising wireless nodes covering from home to larger urban and metropolitan areas. An excellent example of mesh networks is Community Network(s) (CNs). A CN is a (wireless) networking mesh designed by a district of people, principally to deal with the circumstance of the digital gap.

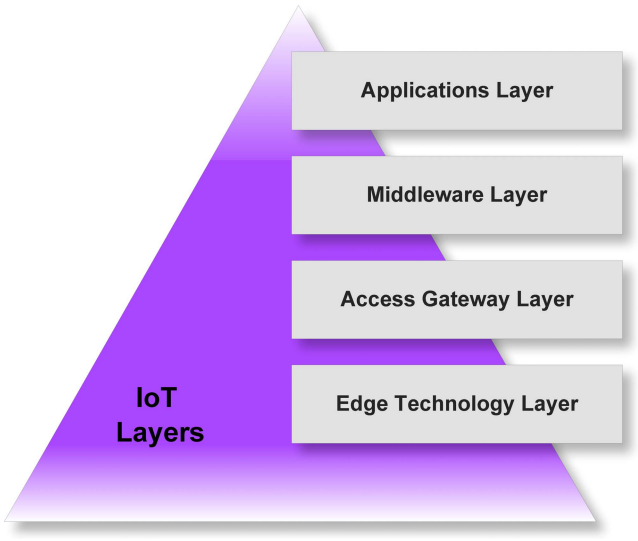


FIGURE 2. The IoT architecture layers.

In this paper, we will try to utilize these networks as a fundamental infrastructure for a viable distributed wireless network, both depending on blockchain's and being applicable for IoT.

B. THE IoT VISION: BACKGROUND AND ARCHITECTURE OVERVIEW

IoT is a state-of-the-art technology trend that is gaining significant popularity based on current wireless telecommunications [8]. The essential nucleus novelty of this conception is its omnipresence in our daily world through numerous things, entities, or objects, such as Radio-Frequency Identification (RFID) tags, activators, sensors, (inter)connectors, actuators, robotic drones, tablets, mobile (smart) phones, etc., that are able to interconnect, communicate and collaborate for standard functionality [113]. Nowadays, the Internet of Things (IoT) interlinks the Internet World Wide Web with sensors and a plethora of devices, predominantly using IP-based connectivity. Undeniably, the principal benefit of the IoT visualization is the extreme implications it will carry on several sectors of daily life and traits of candidate users, from the private and public sector to our personal life domain [5].

Clearly, from an architecture angle, Internet-of-Things (IoT) leverages several layers, as shown in Figure 2.

The two minor layers commit to data apprehension and acquisition, whereas the two superior layers are mainly accountable for data usage in most applicability scenarios [5]. We base our following definitions to formulate the security & privacy challenges for IoT, per each layer, in the next section(s), with the functions of the layers following next [5]:

1) *Edge technology layer (or perception layer):* This is the lowest layer, which mainly comprises of input

data aggregation components, including wireless sensor networks (WSNs), RFID systems, computer vision devices, cameras, robotic sensors, intelligent terminals, industrial code readers (e.g. Quick-Response Codes and/or Optical Character Recognition systems), electronic data interfaces (EDIs), global positioning systems (GPS), and actuators. These hardware elements offer identification and information data storage (i.e., via RFID tags), data collection (e.g., via smart sensor networks), data processing (i.e., via embedded edge/cloud processors), communications, control, sensing, and actuation (i.e., via intelligent robots). The common, like IoT technologies, are as such:

- *RFID systems:* They are, basically, the elementally crucial components of the IoT system. They activate information transmission through an ultra-mobile device named as an RFID tag. The RFID reader obtains the tag and converts it into a specific application machine-readable type of format.
- *Wireless sensor networks (WSNs):* WSNs are comprised of a huge number of sensing nodes, which directly address the sensing data outputs to explicit nodes (sinks).

2) *Access gateway layer:* This particular layer is responsible for information manipulation, as well as information transmission, meta-data routing. It directs to the middleware layer all information acquired from the edge layer, using conventional telecommunications means of technologies like Wi-Fi, Li-Fi, Lo-RA, Ethernet, WSN, GSM, 4G, 5G-LTE, and WiMax.
3) *Middleware layer:* It is a software-defined, composable super-set of sub-layers, intermixed amid the technological and experience levels. The MW layer's main goal is to perform information abstraction and to hide. The IoT technology often follows the Service Oriented Architecture (SOA) flavor. The adoption of the SOA standards provides the room for deconstructing complicated and monolithic systems into simpler applications, comprising an environment of flexible, atomic, and solid components. [1]
4) *Applications layer:* This is the uppermost layer. It is mainly authorized for the carriage of numerous applications to versatile IoT users, with concurrent Quality of Service (QoS), super cloud/edge-computing technologies, Big Data mining, machine-to-machine (M2M) type of communications and services. It also holds any mandatory application user interface (GUI) properties.

C. RATIONALE FOR BLOCKCHAIN INTEGRATION IN IoT

The IoT poses as a new disruptive technology, *driving for the Industry 4.0 revolution*, transforming manual processes into fully automated, scalable, and intelligent. By enabling massive Big Data, and numerous smart appliances and sensors, the IoT manages to improve standards of living through complete digitization of everyday life. Recent advances in Cloud Computing have given another flexible boost to the deployment of IoT. However, this cloud-Internet-of-Things integration still remains unproven, despite being promising.

It is aforementioned that cloud services tend to become unreliable in terms of cybersecurity, however, the introduction and confluence between Blockchain and IoT can enrich the latter by offering a trusted, online sharing service, where whole data source(s) are trustworthy and fully transactioned. These sources of data can become identified and located anytime, whereas this exact data remains unchanged over time, thereby rising its security levels. Such security provisioning can be also scaled into multi-sharing and multi-participant scenarios. Any potential data leakage at any time and location point of the protocol operation can be technically retrieved, thus, it is indisputable that blockchain technology is strongly characterized as the key solution to providing scalability, privacy, trust, and reliability context inside the problems related to the IoT environment.

The technical improvements that this confluence can create include (but are not limited to) [71]:

- **identity/authentication:** utilizing a common blockchain system infrastructure, participants are able to locate and name every single (IoT) device. Data that is fed into the previous system is fully logged and immutable, as well as uniquely identifiable; as a result, Authentication, Authorization, and Accountability (AAA) are being delivered in a *trusted* manner by the blockchain for IoT applications, representing a huge improvement in the IoT paradigm and its participants.
- **decentralization & scalability:** the smooth transition from centralized system architecture, to a Peer-to-Peer (P2P) decentralized one, will eventually avoid single points of failure and threshold bottlenecks. Fault tolerance and system scalability is an example of such improvement results. Monopoly instances where a few big companies possess and store information of a huge number of people are easier to prevent, now, essentially, democratizing the blockchain-IoT confluence.
- **autonomy:** blockchain vision powers the next-generation of application features, making it feasible to deploy, build and commercialize assets and cloud hardware as a service. IoT can become more device and layer agnostic since the whole construct (blockchain/IoT) is completely serverless.
- **cybersecurity/reliability/trust:** as mentioned earlier IoT data is immutable during the ledger protocol operation(s). Since IoT is so sensible in terms of data functions integrity and accountability issues, the blockchain technology can verify such transactions, and their participants (hardware IoT sensors), and provide higher transparency. The blockchain-based IoT devices can ensure the security and confidentiality of the information and the communication messages provided *(1) they are stored as blockchain transactions, (2) validated by smart contracts, (3) and standardized by IoT security alliances*. Finally, within such a reassuring context,

micro-transactions and micro-payments can be viable, between various peers, safe, and optimized, driving the economy of the IoT ecosystem even further.

- **(IoT) security-by-design:** now taking further advantage of highly secure storage on the blockchain, firmware and middleware code (e.g. update patches) can be pushed to IoT devices securely and safely. Even the tracking of pushes, updates, and ''patching'' events is more confident than ever before, thus helping manufacturers to increase their functionality.

Despite the ameliorations offered by the blockchain within the IoT, there still exist several technical challenges to consider, for instance, the level of depth of integration of the decentralized platform within the IoT layers, energy consumption problems (i.e. the IoT is lightweight, by nature), as well as reusability and scalability issues. From a pure security standard perspective, blockchain, and explicitly its consensus protocol which typically causes its greatest bottleneck, could be readapted to provide better security, reduce latencies and increase the bandwidth, thereby helping to achieve a more efficient transition to the IoT.

D. GENERAL LEDGER-BASED IoT PLATFORMS

Quite recently, dozens of blockchain platforms have emerged, due to the several prospects of the confluent technologies that offer. Although this Survey focuses on the *IOTA cryptocurrency*, this particular section briefly summarizes the most typically met applications & platforms that aim to merge the IoT and the blockchain.

Besides Bitcoin & IOTA protocols, another perhaps more popular and IoT-compatible ledger coin has been Ethereum [72]. Ethereum is a pioneer blockchain in including smart contracts. It is basically a blockchain combination of an embedded programming language (Solidity), as well as a consensus-based virtual machine, executing worldwide (Ethereum Virtual Machine EVM). This adoption of smart contracts, its disassociation from cryptocurrencies, the high level of integration, and its open community make Ethereum flexible for most IoT applications.

Hyperledger [73] has further met a great reputation in the field. Hyperledger is, practically, an open-source distributed platform among which many projects are currently being executed and without any commercialized cryptocurrency dependence. By using generic programming languages and IBM's online cloud platforms (IBM Watson IoT Platform, and/or IBM Bluemix), IoT data can be supported, embedded, and integrated inside the blockchain quite easily. The most typical benefit of this ledger platform is its high speed.

The Multichain [78] system deploys private blockchains. Multichain extends the conventional blockchain API with new traits and functionalities, in order to allow the management of portfolios, assets, and transactional permissions in a private-centric manner. It provides a command-line user interface to interact with the tool, and network integration by using programming languages such as Java, Node.js, Ruby, and C#. Its proof of concept compiles for 64-bit architectures.

TABLE 1. IoT-enabled blockchain solutions.

Blockchain platform	Consensus	Smart contracts
Ethereum [72]	PoS	yes
Hyperledger Fabric [73]	PBTF/SIEVE	yes
Multichain [78]	PBTF	yes
Litecoin [74]	Scrypt	no
Lisk [79]	DPoS	yes
Quorum [75]	Multiple	yes
HDAC [76]	ePoW, Trust-based	yes
IOTA [16]	Proof of Work (PoW)/Proof of Stake (PoS)	yes

Litecoin [74] is typically identical to Bitcoin, but has much faster transactions, lower confirmation times, and improved storage efficacy, due to the main minimization of the block generation time (over 5 times less). Furthermore, its proof of work is founded on a lower computationally required mathematical library, more applicable for the IoT.

Lisk [79] provides a blockchain mechanism platform where subdomains of blockchains and chains can be deployed with customized decentralized applications and cryptocurrencies to use. Known for its interoperability, reliance on javascript, and flexibility, Lisk is collaborating with Chain of Things to testify whether the blockchain technology is efficient, in terms of cybersecurity, within IoT.

Quorum [75] is a ledger-based platform that offers a full financial services industry encompassed with a licensed realization of Ethereum with full support for transactional and contract privacy. It permits multiple consensus mechanism(s) and aims for data privacy via segmentation and cryptographic techniques. Recently, the Quorum platform has been integrating ZeroCash technology to make all identifiable meta-information of a transaction oblivious.

HDAC [76] is basically an IoT contract as well as an M2M (Machine-to-Machine) type transactional platform founded on Blockchain, under current implementation. The HDAC is a brand new concept framework scheduled to be launched as soon as possible, possessing private & public blockchains and a quantum (true) random number generator to guarantee the security of these transactions.

Table 1 shows a brief comparison of the IoT-managed blockchain protocols for establishing IoT applications. Although out of the scope of this Survey, due to our main focus on IOTA, we can comprehend that the corresponding presence of smart contract(s) among such previous protocols **ensures** high security for the IoT/blockchain paradigm; *however we plan to establish a more comparative research analysis between those different ledger-based technologies as part of the future work*.

E. IOTA: DAG-BASED LEDGER PLATFORM FOR IoT

Since the Bitcoin protocol was conferred in 2008, there have been emerging plentiful Blockchain-based protocols and technologies (PoWs), relaying on application scenarios and deployments, e.g., *Bitcoin*, like *Ethereum*, *Tether*, and *Litecoin*. All contribute to the same design fundamentals of the generic Protocol [6].

A relatively recent and versatile research attempt lies in the distributed ledger scheme protocol is known as the

Tangle [16], which is utilized in the IOTA (ledger) cryptocoin to fully log P2P transactions. Primarily, the Tangle is nothing more than a Directed Acyclic Graph (DAG), where a vertex defining a transaction holds two ancestors, i.e. the transactions it acknowledges. Based on the suggested Protocol, a PoW or a PoS (alternate solvability of the consensus-based on internal properties, like the number of owned tokens), must be accomplished when accumulating a transaction to the Tangle. This should prevent an attacker from engaging in network spamming. Nevertheless, it is still not yet clear the amount of security impact PoW/PoS offers the Tangle. This is a future research scope that needs to be investigated as described in the later sections.

Whenever a novel transaction is added to the Tangle, it references two previous unlogged (unconfirmed) transactions, called *tips*. The algorithm that selects the two tips is named the Tip Selection Algorithm (TSA). The TSA is the most primitive part of the Protocol as it is utilized by the ledger participants to determine, from two "competitive" transactions which are validated. It is also the most crucial phase for the participants to achieve consensus. The TSA commonly used in the IOTA standard utilizes the PoW included in each transaction to choose the two tips. There exist several instances of TSA variations in the literature. Some include Monte Carlo Markov Chain (MCMC) random walks inside the DAG, while others rely on stochastic processing models to identify and reduce the computational lag for the average number of unconfirmed transactions (called tips). All of these TSA case studies seem to correspond to a Nash equilibrium [20]. Next, we briefly describe the model analysis for the Tangle, in terms of its most defining mathematical characteristics [15].

1) THE NETWORK

We acknowledge a structural set of N processes, denoted as nodes, that are completely interconnected (fully meshed). Each node is able to transmit a notification (message) to all rest nodes. We pre-define that nodes are enabled synchronously. The time plane dimension is discrete, and at every time point fragment, called a round, a node processes the notifications transmitted by the rest nodes in the former round, deploys the Tangle protocol, and, if necessary, can then direct a message to all rest nodes. Whenever a node directs a message, all the other nodes acquire it in the preceding round. There is a threshold bound on the maximum capacity of the messages as long as the nodes obey the Protocol legitimately and securely.

2) THE DAG

As mentioned previously, we describe a specific type of distributed ledger scheme named as the Tangle, which is a Direct Acyclic Graph (DAG). Each node u compensates at each specific round r a local DAG G_r^u (or simply G_r or G), where each vertex, called a site, defines a ledger-based transaction. Each site possesses two parents (sometimes equal) in the DAG. We namely define a site as *directly confirming* its mutual parents. All sites to be approved by the parents of a corresponding site are also considered to be confirmed (or non-directly confirmed) by it (see Figure 1). A site that is not yet attested is known as a tip or technically an unconfirmed transaction. There exists, finally, a unique site named genesis that does, indeed, not contain parents and is confirmed by all rest sites. Two sites might also collude with each other; thus, state recognition and awareness are always apparent on the Tangle for all present sites.

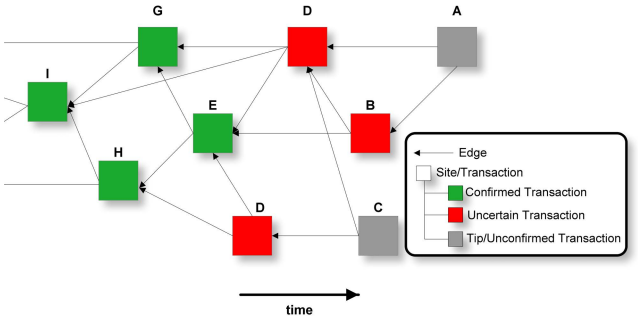


FIGURE 3. An example instance of a Tangle.

In case the Tangle is utilized to log all the monetary credits of a given cryptocurrency (e.g., the IOTA cryptocurrency), then the site defines a transaction for transferring funds from a sender address to a known receiver address, and two sites are considered to be connecting if they make effort to present the same funds to two fundamentally different receivers, i.e., if mutually are deploying transactions that result in a minus balance for the transmitter. During each round, each node may approve one or several transactions. For each transaction, the node chooses among two parents. The pre-signed or confirmed transaction is finalized thereafter as a novel site in the DAG. Then, ultimately, that node broadcasts that site to all other nodes.

3) WEIGHT AND HASHING POWER

After a transaction is approved or the site is aggregated to the graph, a negligible proof of work (PoW) is computed. The difficulty or computational complexity of this exact PoW is determined by the weight of the site. Initially, this PoW is aggregated to the Protocol, to disallow a node from spamming a considerable sequence of transactions. It has been mathematically proven that with the PoW, IOTA network spamming demands a considerable amount of processing power, thus driving it even more complicated for malefic users to undermine the security and availability of the Tangle.

Several underlying *Security, Privacy*, and *Confidentiality* assumptions emerge from the Tangle concept. There are also several attack scenarios, vectors, and threat models that are meant to compromise the ledger's reliability to allow the attacker to mistakenly receive *double* payment and rattle the availability status of the network inside the non-financial transactions-based IOTA applications. We discuss, tabulate, and formulate these issues in the following sections.

III. IOTA SECURITY AND PRIVACY CHALLENGES

IoT itself is a complex system that alongside with ledger-capable distributed wireless networks imposes a new dimensionality of complexity to the environment for high-tech applications. To adequately cover the necessity of utilizing DLT for IoT, we investigate which of the following *Security Classes* and requirements are most crucial.

- **Confidentiality:** Confidentiality refers to the collection of measures that are taken to ensure that sensitive data is being kept secret, with a scope limited as much as possible, and being made unreachable by malefic users. It also makes sure that the rightful data owner of the information may have access to it.
- **Integrity:** Integrity clarifies that data communicated remains idle and trustworthy. It includes retaining the accuracy, integrity, trustworthiness, and consistency of information over the data life-cycle. In transit, the information should be never compromised or forged by unauthorized users.
- **Availability:** Availability indicates that the data is accessible to authorized participants. This also reflects the fact that accessibility by authorized data owners should *always* be applicable. Data access, service provisioning, functionality, maintainability, and account access are a few examples included within this scope.
- **Accountability:** The question that arises when we co-deploy key game-changing technologies like IoT and DLT in wireless networks is who is to blame for when a non-technical fault or security attack takes place. Is the IoT vendor mainly responsible, the ledger regulators, or the network maintainability operators themselves? *Security-by-Experience* and *Security-by-Default* are perhaps the only addressed solutions to this issue.
- **Scalability:** Since there are numerous types of heterogeneous devices co-deployed together upon the IoT platform, it is challenging to offer the same security agreement alongside the entire network.
- **Manageability:** It is a challenging task to manipulate the access of all the devices, which leads to many authority ownership problems.
- **Reliability:** As IoT comprises a diversified network, it is trivial to authorize the reliability of all data sources likewise in the case of data attacks *(e.g. the man in the middle attack)*.
- **Capability:** Reduced size of memory and a limited amount of computational resources make it complicated to prototype any security algorithm. Lightweight Cryptography comes in as a reliable solution for this challenge.
- **Privacy:** Protecting and securely ensuring the data information of participants from any exposure and leakage of data in the hands of undesirable users is perhaps a mandatory task. Policy regulations from national/international laws apply here, thus making the challenge greater. Blockchain technology has been awarded its yet vast popularity due to its ability to deliver privacy over a non-centralized network.

There exist many other challenges, namely defined as security (sub)classes, due to the DLT paradigms; e.g., *Collective Verification* where a third (trusted) party validator should be present to verify the IoT device-related TXs, *Anonymity* where by using Asymmetric Cryptography it is virtually hard to detect the real identity of a DLT assigned real user, and *Autonomy* where no individual node or party can **atomically** manipulate or control the ledger, thus storing, transferring or updating any data in the Blockchain itself [9].

In the next follow-up, we thoroughly investigate the main technical provocations from the emerging co-utilization of IoT and Direct Acyclic Graph (DAG), mainly in terms of *Security and Privacy*.

A. SECURITY VS. ENERGY COST

DLT demands a consensus algorithm to reassure the agreement on the identification, validation, and verification in a decentralized system. However, the conventional Blockchain is power-hungry due to its high computational complexity. Thus, conventional Blockchain is suitable for crypto-currencies mining, and due to this high polynomial complexity (e.g., double-hashing function), it makes security feasible on the one hand but energy efficiency harder on the other. The computation demands additive graphics processor units (GPUs), due to high-end physical hardware needs. Consequently, the monetary expenditure is the number one draw-down of paramount significance while implementing Blockchain in versatile systems, *including the lightweight nature of the IoT instance*.

B. DAG-BASED LEDGER ADAPTATION

IoT ecosystems require resource-limited end physical devices where ledger-based cryptocurrency models can be customized for IoT applications. Leveraging DAG architecture with IoT meets some trivial concerns as conventional ones demand extremely highly parameterized computing resources, quite irregular to the true vision of IoT, which is lightweight. Therefore, adaption or cohabitation requires further modification in the DAG-based ledger framework to confront the IoT ecosystems easily. Primarily, consensus model(s) demand further alterations as current ones are very expensive in terms of computational resources and energy consumption metrics. Since IOTA and IoT are non-centralized systems, the implementation goals, area scopes, and breakthroughs are more versatile. However, leveraging the opportunities, challenges and high prospects of leveraging the ledger in IoT motivates to redesign the adaptive DAG consensus model as the ''chain'' provides not only incremental privacy & security but also restricts the needs for a centralized fully-trusted (central) management system which is less fault-prone and scalable. In simple words, we can research the benefits of the ''chain'' (its strong security and privacy levels and distributed nature) along with the ''IoT'' case (its flexibility, simplicity, and high scalability behavior).

C. IOTA INTEGRATION WITH IoT

DAG and Internet-of-Things (IoT) are revolutionary technologies that will have a key role in future meshed networks. Both are fundamentally different in terms of scope, nature, and implementation methodologies; however, they need to, and they can be integrated to accomplish more feasible, secure, private, and agile systems. In most DLT-IoT-based architectures, several crucial traits like enhanced trustworthiness, fault tolerance aptitude, higher scalability, faster and more effective processes, as well as scalability exist [15], [16], and [23].

D. SECURITY IN DAG-BASED LEDGER IoT ECOSYSTEM

The configuration of adapted IoT systems is prone to security and privacy risks. The ledger can make the cybersecurity of these specific IoT devices more robust by conserving critically sensitive security data they possess, as well as other embedded security tokens. Cyber-physical systems (CPS) maintain crucial security and privacy issues explicitly during machine-to-machine (M2M) type communications. A state-of-the-art ledger structure has been architectured amid the public domain and the private domain to confront cybersecurity matters [11]. Finally, security, trust, and transparency not needing a third (trusted) party, or authority, is the first bonus asset of co-developing DLT (IOTA) with IoT.

E. PRIVACY VS. CONFIDENTIALITY

To successfully retain the privacy issue, several symmetric cryptosystems and asymmetric as well as cryptographic tokenization have widely been utilized in all networking systems. Therefore, in the paradigm of the IoT ecosystem, cryptographic encryption is the conventional manner of reassuring data confidentiality during device interaction. In the Blockchain-based system, node parties can quite easily broadcast the identity of the rest of the nodes within a networking system, and TXs data is possible to become encrypted utilizing a public key or even with a (from before) shared private key. The number of IoT devices per user is so vast that it demands even more sophisticated cybersecurity measurements. The solution for data preservation in the BC-IoT instance, hence, could rely on the Attribute-based encryption (ABE) methodologies, which were adapted to marginally modify the ''chain'' protocol to guarantee better privacy [12].

F. INTEGRITY

In the DAG-based IoT ecosystem(s), the hash result(s) of versatile fields of a TX block(s) is a decent method in order to retain information integrity. In [13], messages are securely signed within the associated private key of the adjacent peer to reassure trust as well as information integrity. Proof of Trust (PoT) has been widely utilized in a multi-tier IoT ecosystem(s) for increased data integrity verification and validation. A framework based on the DLT-IoT technique is well depicted in [14], which offers better-trusted data integrity authentication, especially for the IoT Big Data of mutually both the data creators/owners and data consumers. This framework will not depend on third-party validations for the ad-hoc verification of data integrity, which might decrease credibility. Furthermore, it offers other merits such as the preservation of consuming data with their data consumers and the instantiating of pay-per-transaction data integrity as-a-service (AS).

G. AVAILABILITY

Availability is a major challenge in the DAG-IoT co-existence. It merely relies on manipulating the requests from solely authorized nodes in a fully trusted environment so that benign, or unfavorable, requests could be neglected. Whereas in IoT, DDoS attacks are mainly very typical and easy to launch, in the ledger environment is nearly infeasible provided the participating peers in such a network are authenticated and properly authorized, thus turning it impractical to log in to the network by ''pretension'' attempts.

H. AUTHENTICATION

Due to the decentralization, the ''chain'' delivers *default authentication* simply as the total environment is decentralized, and every unique node or associated in the network is atomically verified by other members independently. Proving and ensuring Authentication in IoT instances is more trivial and semantically insecure. Thus, there exist several research contributions that distinguish and authenticate nodes in the ledger-based IoT ecosystem. For example, a node could use a ticket during start-up to self-authenticate and a special object ID securely signed with its private key to be used for validation.

I. AUTHORIZATION

IoT devices must hold strong and secure identities and user ownership properties, which are presently not offered or provided by default by their manufacturers. Many ''chain''-based IoT lightweight frameworks have been studied to provide registration-confirmation systems through which a terminal will get a unique ID for authorization. Moreover, these models also re-assure reduced monetary costing for services using an atomic contract-based charging system that is autonomous of versatile applications and infrastructure.

J. NON-REPUDIATION AND ACCESS-CONTROL

A trusted third party is always a necessity to ensure correct access control verification for the exponentially increasing IoT devices. The essence of non-repudiation correlates to the transparency of the transaction tracking that is verified by both parties. In a non-repudiated ledger-based IoT system, all the transactions are logged, stored, and recorded in the public ledger domain so that, eventually, no one could negate the fulfillment of a standalone transaction.

IV. IOTA COMPREHENSIVE SECURITY ANALYSIS

Nonetheless, there is ongoing research work related to the security & privacy implications of applying Blockchain

technologies inside the Internet-of-Things (IoT). Interacting the ledger with IoT seems eminent in the banking sector, software development, real estate, and smart grid, whereas quite recently very important political bodies have started to spotlight the IOTA digital prospects [102]. Quite similarly, though, nearly all aforementioned surveys do not cover the wider aspect of the Blockchain-IoT true interaction and stay mainly on particular Cybersecurity concerns. We tend to select some of those specific that tend to provide explicit research contribution.

Authors in [103] highlight the systematic security attacks and vectors that pose threat inside the ledger-IoT interoperability, whereas they propose security requirements, countermeasures, and open challenges. In [44], the authors implement a novel decentralized mixing protocol for the IOTA digital ledger that combines the decryption of mixnets and multi-signatures. They claim their system can guarantee security and privacy even in the presence of benign entities in the infrastructure. Authors in [104] refer to a customized Blockchain solution for Internet-of-Things by overriding the structural deficiencies of conventional IoT when applied inside the ledger paradigm. In [29], they discuss the overall security, privacy, and trust issues emerging on the practicality concerns of the Blockchain universe. An Authentication and Access Control (AAC) reference, together with an additional smart contract taxonomy illustration is being depicted in [105]. The authors in [106] address very frequent types of security vulnerabilities and threats on the IOTA protocol and utilize the Common Vulnerability Scoring System (CVSS v3.0) to practically examine their true potential. Inside [27], their authors propose an alternative system approach while interacting IOTA with the Blockchain to reduce the transactional fees and power processing costs while peering at the ledger network. In a recent article, [107], an attempt to project the system evolution from Internet-of-Everything to IoT/Ledger is being performed, mainly from the application & applicability layer. The research article in [108] addresses the key security attacks as well as their security solutions that will help, according to the authors, establish stronger Blockchain systems. The confluence of the Internet of Drones (IoDT), artificial intelligence (AI), and blockchain is being carefully analyzed in most recent article [111]. The author's implemented novelty relies on monitoring pandemic outbreaks, with an additional two-phase lightweight security mechanism being adapted for *authorization* purposes. Another most latest work, in [110], mentions federated learning-based blockchain intervention for authentication purposes with strong differential-based privacy presence. Finally, authors in [109] invest more in the *Privacy* concerns of the Blockchain with the suggestion of a privacy-enhancing content erasure mechanism that aims to increase the anonymization concept of the ledger.

Illustratively, Tables 2 and 3 depict our comprehensive analysis in terms of Cybersecurity, starting from (a) the conventional centralized IoT, (b) the promise of (classical) Blockchain/IoT interaction, (c) the migration, finally, or making of the next transition to the new IOTA era, but also (d) the proposal of several challenges worth of future research investigation (see Table 3, column 4). It is worth noticing the two tables have an inheritance of transition or technology migration property; while *Blockchain Solutions* from the Table 2 seem to provide some benefits in terms of the cryptographic consistency of the Internet-of-Things inside the ledger, these solutions still lack paramount interoperability and performance trade-offs already mentioned in earlier sections. Thus, Table 3 addresses the above limitations of the novel IOTA concept.

Novel challenges from the next ledger generation, such as threats and exploits, are presented in Table 2, together with security mitigations *per requirement*. However, because our study analysis is exhaustive, we can identify new cybersecurity directions that remain unattended by the research community for the DAG-based ledger IoT. These types of deficiencies are worth addressing in the future by improving hashing functionalities, like the *Curl* primitive, and the dynamic network conditions of the DAG, and are selecting the most optimal (Game-Theoretic) consensus algorithm or Tangle for this ledger-based IOTA.

Surplus, by attaching typical nature-specific security and privacy challenges that are apparent to the Internet-of-Things, Table 2 aims to enlighten further several other cybersecurity aspects. IoT devices often have low reconfigurability options or none at all. Modifications in the DLT infrastructure and protocols may turn IoT devices to either become detached from the distributed ledger or to selectively have limited functionality. A deprecated IoT system will frequently lack support from an updated *patch* version of the DLT, other security concerns arise from the non-updated condition, so *reliability* and *trust* for DLT-IoT is at stake. Power is an important issue in IoT. Low-power IoT is unable to compensate or process the full distributed ledger. From the security point of view, classical IoT possesses distributed traits, and hence prone to DDoS attacks it requires third parties as trusted nodes of (inter)validation.

To mitigate those intrinsic IoT defects, the traditional, or ''decentralized'' ledger blockchain solutions can offer many security improvements. The ledger provides strong auditability and trackability possibilities through complete full transactional logging features. Together with the smart contract and more vigorous decentralized verification via digital signatures, data integrity, privacy, and a lack of reliance on third parties from IoT devices improve significantly. Furthermore, as seen in Table 2, whenever an attacking IoT device tries to penetrate the whole network on the ledger approach, it cannot be achieved as it immediately gets detected (point of attack) and thrown out of the Blockchain. Finally, resource utilization, either in an idle system state or attack state, is better stochastically normalized in the distributed ledger rather than the centralized Internet-of-Things. This can have security and privacy benefits for the whole system and the IoT device itself.

TABLE 2. Summary of weaknesses of IoT and (traditional) blockchain solutions.

Requirement (per IoT layer)	Deficiencies of IoT	Blockchain Solutions
Confidentiality	• Maladministration of user data • Control of discoveries in a particular networking direction • Message exchange is achieved through third party or edge/cloud	• Numerous versatile lightweight private and public-key encryption systems for privacy of all ledger transactions. • Trackability • Immutability: once a unique transaction is logged, cannot be modified, detached or removed • Exploit smart contracts for highly secure message communication • Node message exchanges takes place equivalently as financial transactions in bitcoin.
Integrity	• Personally identifiable information (PII) can be leaked,e.g., through profiling • No authorization and data integrity technique(s)	• Proof of Trust is another efficient solution in order to verify integrity in complex systems. • Collective verification introduced via consensus methodologies • Tamper resistance – each unique node holds clone copies of each data • Ability to verify upon malicious nodes • Anonymity of personal private data achieved by secure cryptographic merging of nodes • Confidentiality is preserved analogous to securing identity and monetary balance reports in bitcoin.
Availability	• High chance of computing/networking bottleneck • One sole malicious node can computationally rattle the whole network • IoT small-sized devices tend to become prone to DDoS attacks, data forging and remote based hijacking. • Since, current infrastructure of IoT is heavily reliant on edge/cloud, thence high chance of servers dropping down or cooling.	• Availability is maintained through idle authentication and user validation: benign auditors cannot initiate possible attacks by logging inside the network. • Interlocked IoT devices • When data breach on/out of one terminal, that device is removed out of Blockchain • Utilizing reservations of all meshed participating nodes and neglecting one-to-many and many-to one traffic flows. • Transactions are on a set of devices to hold similar information • A faulty node can possibly join in or get out of the system instantaneously.
Authentication	• Depends on trusted third party (TTP), or validator(s).	• BC provides verification in non-centralized system by recognizing stored cryptographic keys in a transactional procedure while being fully logged in the public ledger. • Authentication can also be full-filled using ticket or tokenization management system. • Cryptographically securely signed logged transactions • Verification of the digital secure signatures • Trust • Mitigating Man-in-the-middle as well as replay attack.
Authorization	• No authorization and data integrity method(s).	• Registration management processes in BC, policy headers and shared secret keys offer adequate authorization for present IoT ecosystem(s). • Collective verification via versatile consensus mechanisms • Tamper resistance – each unique node stores identical (clone) copies of data • Ability to confirm on non-legitimate nodes.
Anonymity	• Leakage of user's identity & sensitive information before release of Big Data analysis.	• Introduction of privacy preserving K-Anonymity technique(s) [49].

TABLE 3. IOTA security and privacy considerations.

Requirement	Attacks	Solutions	Limitations/Gaps/Challenges	References
Integrity	• Collision attacks • Chosen-Message Attack on IOTA's Signature Scheme (ISS) • Hash-function based attacks • Signature forgery attacks	• Calibrating input space of non-normalized chunks onto the output space of legitimate, normalized chunks. • Adjusted hash value when normalization procedure stops • Increasing actual entropy (and security) more than the upper bound of hash-function brute force resistance.	• IOTA ISS possesses generically low hash resistance against generic collision attacks. • ISS normalization process is prone to differential cryptanalysis based attacks. • The chosen-message attack model is incognito to the background of the complete IOTA network • The "even most valid attacks" would not succeed on the live IOTA network deployment due to the unspecified "protection mechanisms" in the closed-source coordinator. • Any closed-source IOTA coordinator would safeguard the IOTA network from vulnerabilities.	[17]
	• IOTA replay attacks: prolifing users IOTAs by 'replaying' transaction chunks. • IOTA 'chain replays'. • Brute force attempts against IOTA: an attacker can create transactions for a deterministic seed. • IOTA replay attacks using past transaction bundles.	• Keep logs of the unique hash of each confirmed transaction bundle and permit one instance of a bundle hash in a (sub)tangle. • An IOTA network node should confirm each incoming transaction to identify if their hash is already recorded in the tangle.	• IOTA is based often on reusable addresses (replay-attack vulnerability). • When a vulnerable address does not contain enough credits for a transaction to be replayed will enable "replaying attacks". • Address reuse is not implemented by default in IOTA. • IOTA trust is stronger than the Blockchain: if IOTA cannot secure funds, it will not become trusted.	[18]
Anonymity	• Degree of IOTA deanonymisation is growing over time: attackers gather more system related information than the systemic entropy itself. • Privacy risks & concerns for IOTA transactions and users sensitive data.	• IOTA development team has built the tangle on the ledger quantum-resistant. • Masked Authentication Messaging usage provides a tentative solution to privacy concerns. • Despite full historical backlogging and tracing of the tangle, only the last class of tokens may be considered potentially uncorrupted by identifiable addresses. • Masking an IP address from other nodes makes anonymity more feasible. • Utilization of Privacy-Enhancing Protocols for IOTA: CoinJoin, CoinShuffle, Centralised Mixers, CoinSwap, Blackbytes, Merge Avoidance, Zero-Knowledge Proofs and Ring Signatures.	• IOTA's usage of hash-based signatures reduces protocol-enhancing means based on elliptic curve and public-key cryptography. • The requirement for a lightweight and scalable encryption scheme further mitigates the solution (anonymization) space. • IOTA has zero fees and thus makes non-centralised protocols difficult to build low resistance to a Sybil attack.	[19]
Confidentiality	• IOTA's hash function (called Curl) is prone to quantum attacks. • Splitting Attacks. • Prone to double-spending attacks. • Possibility to forge signatures on IOTA payments regardless of the Coordinator.	• The tangle Coordinator, which serves as a single administrator that signs the latest good state of the system enhances IOTA's Trust. • Better Nash equilibrium [20] achieved through more efficient and secure PoWs. • The Coordinator is undocumented or closed-source.	• Low number of users in a distributed ledger network can lead to slower tip approval speeds and reduced security. • No bootstrapping techniques applied before, and no trusted parties involved (Coordinator) in the generic version of the tangle. • IOTA's signature scheme is not secure against the Existential Unforgeability under a Chosen Message Attack (EU-CMA). • Low security resistance to Birthday attacks.	[20]
	• Padding Attacks. • Zero-Extension Full-State Collision. • A Related Digest Attack. • A Constructive Collision Attack.	• Curl's Collision Resistance is mandatory for the EU-CMA security of its signature scheme. • New variations of the sponge functions absorb and transform should/can be applied.	• IOTA curl signatures operate on the hashes of transaction bundles, rather than on the bundles themselves. • Polynomial time available for the adversary to produce a valid signature. • Existential forgery and chosen message attacks seem feasible to deploy against the tangle.	[21]
Authentication	• Preimage attacks. • Generating the channel ID from the channel key is usually trivial for subscribers. • Broadcaster can remove access from future messages in their channel at anypoint in time by modifying the authorization secret key.	• Use of Authenticated Data Structures. • Merkle Hash Technique utilization. • One-Time Signatures as well as the Merkle Signature Scheme can be deployed.	• Masked Authenticated Messaging (MAM) vulnerabilities still exist on the tangle channel. • Value-based transactions on decentralized ledgers are typically pseudonymous. • Trade-off between authenticated-based security levels of the tangle & performance feasibility, especially for the IoT.	[22]
Availability	• Parasite Chain Attack.	• Resistance to Parasite Chain Attacks: modification to the Monte Carlo Markov Chain (MCMC) algorithm to mitigate the efficacy of double spending attacks and same time permitting us to maintain a wide Tangle and low chance of orphaned transactions.	• No trusted validators on generic tangle to prevent parasite chain attacks. • Double spending attacks vulnerabilities. • Still on-going research efforts to identify optimal parameters of cumulative weight inside the Tangle to prevent double spending attacks.	[23]
Authorization	• Unauthorized access-based attacks.	• Adoption of Hyperledger architecture [51] for IOTA ledger for authorization in a modular fashion.	• Consensus is reached at a transaction level, when permissioned, or Hyperledger enabled.	[50]

While leveraging IoT with DLT, through the IOTA API, according to several studied literature items, there exist many attack experimentations to either *replay attack, brute force* or *parasite attack* the Tangle. An entirely novel and rising popularity type of attack is on the main (post-quantum) crypt-analysis components of the tangle hashing function (Curl).

Also, during *double-spending attacks*, an attacker wishes to nullify an already recorded transaction and recover the spent money back. Table 2 illuminates the security solutions for these exploitations against the Tangle, *i.e. corresponding cybersecurity frameworks for the mentioned attacks*, as well as limitations and challenges yet to be thoroughly investigated. Based on our analysis of the literature, we can elaborate that while the technical specifications of IOTA's signature scheme remain relatively obscure, we can understand from the references that signatures operate on the hashes of transaction batches, rather than on the previous clusters. This, combined with the mismatch of the Curl's collision resistance property creates an open vulnerability to IOTA for an EU-CMA (Existential Unforgeability Chosen Message Attack). It also appears that these moderate vulnerabilities are not to blame due to the robust parameters used to initialize Curl in the implementation of IOTA, i.e. *permute* or $|r|$, but rather severe intrinsic structural issues with the new variations of the sponge construction functions *absorb* & *transform* [24].

Specifically, as per [17], in Table 3, the authors focus on security attacks on the signature scheme of IOTA (used to validate payments by users). Generically, the IOTA Signature Scheme (ISS) is established on Winternitz One-Time Signatures [80]. The authors achieved fast creation of equal length messages, by using differential cryptanalysis, which hashes to the equally same value with Curl-P-27, thus, being able to break the function's cryptographic collision resistance. They researched collision-type(s) attacks to generate signature forgeries against IOTA. Their cryptanalysis aftermath is that IOTA Curl-P-27 is vulnerable to signature collisions (*however, no currently used for ISS*), and generic attacks, since they had been able, by using 80 cores, to create colliding IOTA micro-payments in a time less than twenty seconds (by average). To mitigate such signature security weaknesses, they adapt a composed hash method and they estimate (new) upper bounds on level one collision resistance in the order magnitude of $E[M] \leq 2^{47.14}$, i.e. they can initiate a brute force using only $E[M]$ such queries (47.14 bits). In [21], the authors adopt an alternative to [17] type of secondary-preimage attack, digest attack, and a constructive full-state collision against Curl hash function, to basically reach the same conclusion; *that Curl is not cryptographically a secure hashing function for the IOTA protocol*. Their further stated conclusion(s), is that despite forgery as well as chosen message attacks seem infeasible to implement in practice, the work in [81] discusses practical scenarios for their physical realizations, thus leaving future limitations, gaps, or challenges to still become addressed. Dealing less with integrity and authentication, and with more relevance to network availability, compared to previous research cryptanalysis, the authors in [23] address the effect of parasite chain attack(s), which aims to disrupt the irreversibility and immutability of the DAG-based ledger. Technically, they build a customized Markov Chain model for the (IOTA) Biased Random Walk (BRW) tip selection algorithm to generate the parasite chain attack. Considering λ to be the rate of arrival of benign transactions, and μ the rate at which the malefic user (attacker) can add new transactions to the (IOTA) parasite chain, their investigated attack model behavior is that as long as $\mu \leq \lambda$, the corresponding attack will always fail. Issues, however, that the authors still leave unaddressed, for future work, would be how to effectively scale their attack mitigation approach to confront higher-order parasite chain attacks, i.e. with higher-order derivatives of the cumulative graph weight of the Tangle.

Overall, [18]–[20], [22], and [50] works are equivalently illustrated in the same table (Table 2), for the purpose of identifying security cryptanalysis results for the IOTA, brief technical & performance analysis of their attack models and mitigation's security frameworks, but also our contribution to spotting any potential security gaps that still remain unresolved.

The novel IOTA Protocol is being divided into three layers: the *network, communication,* and *application layer(s)*. The first (network) layer is responsible for the management of the connections and transmissions packets between DAG nodes. Inside this exact layer auto-discovery peer modules build the connections between nodes based on the gossip protocol. The next (communication) layer stores and constructs the communication information. Basically, the Tangle, or ''the distributed ledger,'' the timestamps, and rate control belong here. Finally, hashing transactional exchange information lay in this layer. The last (application) layer is for any application-related frameworks and control domains that manipulate IOTA messages and objects generated from the two previous lower layer(s). As shown in Figure 4, the full security taxonomy of the IOTA protocol is well correlated with Table 2 security class metrics.

V. PROPOSED SECURITY FRAMEWORK FOR IOTA

To address the open issues in the existing literature with respect to the attacks against blockchain-based IoT systems, we propose our security framework, as shown in Figure 5 to address those limitations. Security parameters indicated in Figure 5 can be used to calculate the Blockchain Vulnerability Index (BVI), which identifies the vulnerability of a blockchain based IoT environment to external threats. This vulnerability index is computed using the parameters collected from blockchain-based IoT environment. By estimating BVI, the performance trend of a blockchain-based IoT environment, from the cybersecurity perspective, can be evaluated. BVI is computed over a specified time frame and can be collated with the benchmark index thresholds as obtained from historical training data. Model training is realized by collecting data, with presence and/or without the presence of attacks, with and/or without control over a long time period. The intra-comparison of the threshold index with the BVI is utilized to activate the response framework in order to secure the blockchain-based IoT environment [82] - [83].

Following are the detailed steps in the design and implementation of the proposed framework.

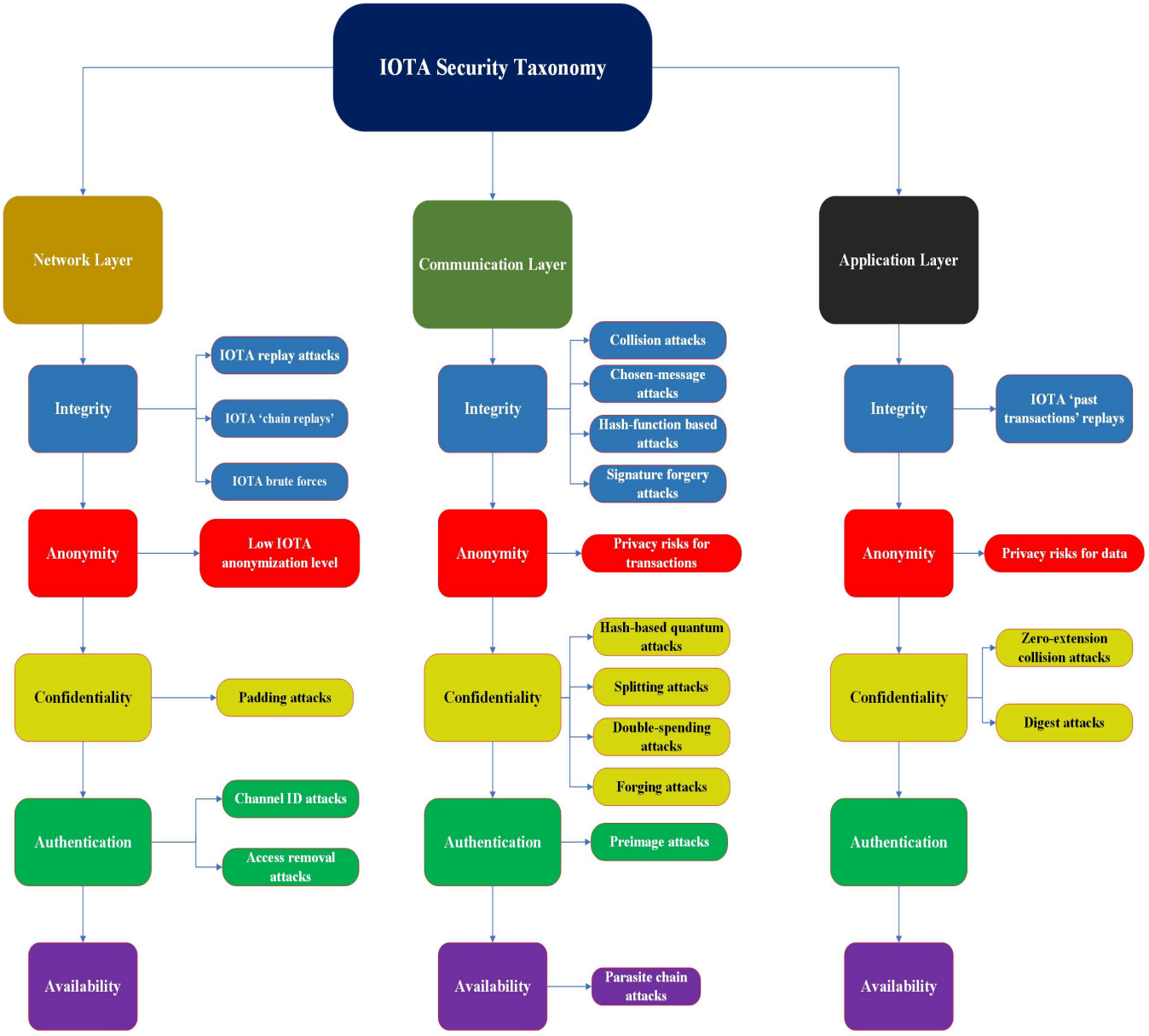


FIGURE 4. IOTA security taxonomy.

Step 1 (Threat Modeling and Data Collection): Threat models for the blockchain-based IoT environment will be implemented in this step. A module for identifying and collecting security threat attack data for the relative threat scenarios/models system would also be implemented in this phase. Blockchain based IoT is represented as a function: $f(x1(t),\ x2(t),\ \ldots\ xn(t),\ v1(t),\ v2(t)\ \ldots\ vn(t),\ m1(t),\ m2(t),\ \ldots\ mn(t),\ k(t),\ u(t))$, where $xn(t)$ represents the most significant attack (sensitive) parameters, $vn(t)$ represents the parameters which are less significant in terms of representing the node(s) vulnerability, $mn(t)$ defines the mobility parameters, $k(t)$ demonstrates the attack and $u(t)$ represents the main control input. $xn'(t)$ depicts the modified values of the most significant attack (sensitive) parameter due to presence of the attack $k(t)$ and the main control input $u(t)$.

Step 2 (Threat Detection): In this step, BVI at a node level is evaluated by the BVI evaluation system using the exact attack sensitive parameters, such as packet drop, energy consumption, processor usage, memory usage, etc., $xn'(t)$ [101]. The computed BVI(t) will then be contrasted with the threshold values of the Blockchain Vulnerability Index BVI'. The BVI limit thresholds (BVI') are derived with the help of the input training dataset, where each record state is labeled.

Step 3 (Response and Protection): Upon detection that a node is vulnerable to a threat, the nodes are prone to the response & protection algorithm [101]. This algorithm isolates the attack, as well as the adversary, and trans-

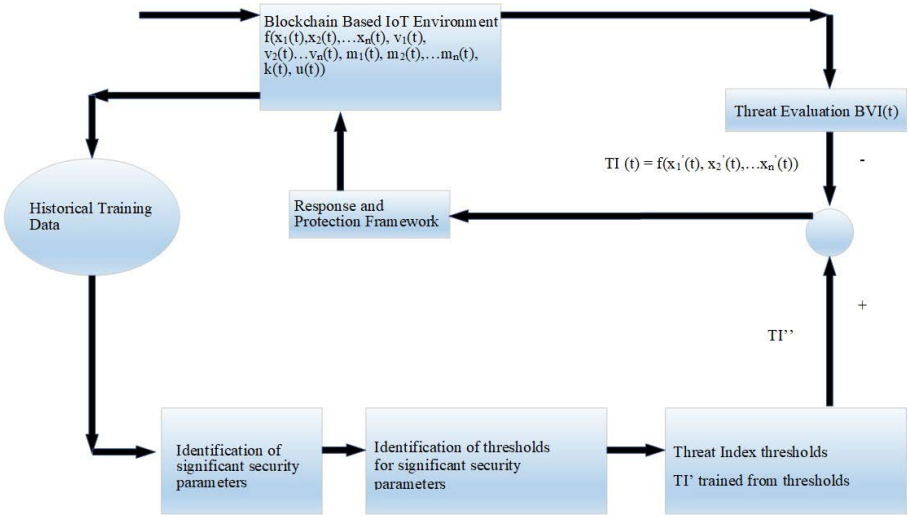


FIGURE 5. Proposed security framework for blockchain based IoT.

mits the control signal $u(t)$ to protect the blockchain-based IoT. The control signal $u(t)$ is versatile depending upon the exact type of the attack. This control signal readjusts the blockchain-based IoT and modifies $f(x1'(t+1), x2'(t+1), \ldots xn'(t+1))$ so that BVI(t+1) achieves the steady normal state. It should, however, be derived that $f(x1'(t+1), x2'(t+1), \ldots xn'(t+1))$ also rely on new attack $k(t+1)$.

Our security framework can be integrated with security tools to the existing IOTA network. These tools are implemented in a decentralized fashion and experimented with to demonstrate their viability.

VI. FUTURE RESEARCH DIRECTIONS

IOTA is the most novel cryptocurrency that deploys distributed ledger technology based on the directed acyclic graph (DAG) data structure. The security of cryptocurrencies almost always tends to be criticized for lower security, degradation of trust, and inheriting malicious operations. Although IOTA systemically and automatically provides resilient security controls, IOTA security is not currently yet thoroughly explored. Many security and privacy issues seem to arise not only in the deployment instances (network configurations) but also inside the very cryptographic building blocks themselves (e.g., hashes), making this transition of IoT from conventional Blockchain ledger to the next generation of DAG-based IOTA more difficult. While we provide concrete security recommendations to address most concerns, the future scope is left for further mitigation analysis from the research community.

In this work, we perform an intensive research case study and analysis using full cybersecurity requirements point of angle for the IOTA, or DAG-based ledger Internet-of-Things cohabitation. Likewise, in our most recent related research publication [101] we prototyped a Machine Learning (ML) approach embedded with a mathematical background formulation technique (*sliding window with interpolation*), alongside a reinforcement-learning agent, that can create security threat indexes based on anomalous resource consumption observation status of each IOTA-Tangle nodes. We also aim to project anomaly detection prediction, based on ML, for mitigating security attacks mentioned earlier against the IOTA. As per theoretical discussions in [112], we estimate a run-time complexity of $O(n^3)$ in our typical DAG-based scenario implementation, i.e. the IoT integration inside IOTA. Our system prototyped solution is scalable and transactive for the IoT paradigm. By leveraging the IOTA protocol, we can find this research approach easy to scale in larger networks and higher number of integrating nodes. It is therefore attested that for the proof of concept our network topology can become integrated in larger and more complex cloud environment scenarios. We can project our full Artificial Intelligence (AI)-enabled deployment framework as shown in Figure 6. The brief description of the logic diagram depicted in Figure 6 are as follows:

- Notably, all functional blocks are callable via enable/disable flags. For example, activation of (Reinforcement-Learning) RL-rule, or not.
- The functional flow of the diagram is rightwise and top-down. Starting from item #1 until item #10.
- Specifically, the master main input is the first red dot on the left part, whereas the master main output is the (dashed) red dot on the (bottom) left part of the schema.
- All green colored boxes are the PROCESSES: Their name corresponds to the file_name of each Python function at the corresponding folder(s).
- All cyan colored boxes are the SUBPROCESSES: e.g. {Block}, or {Stream mode} and {Game(s) Container}.
- The utility function is selecting the functionality among +Anomaly Detection (+with OR +without RL-RULE) OR +Anomaly Prediction (+with OR +without RL-RULE).

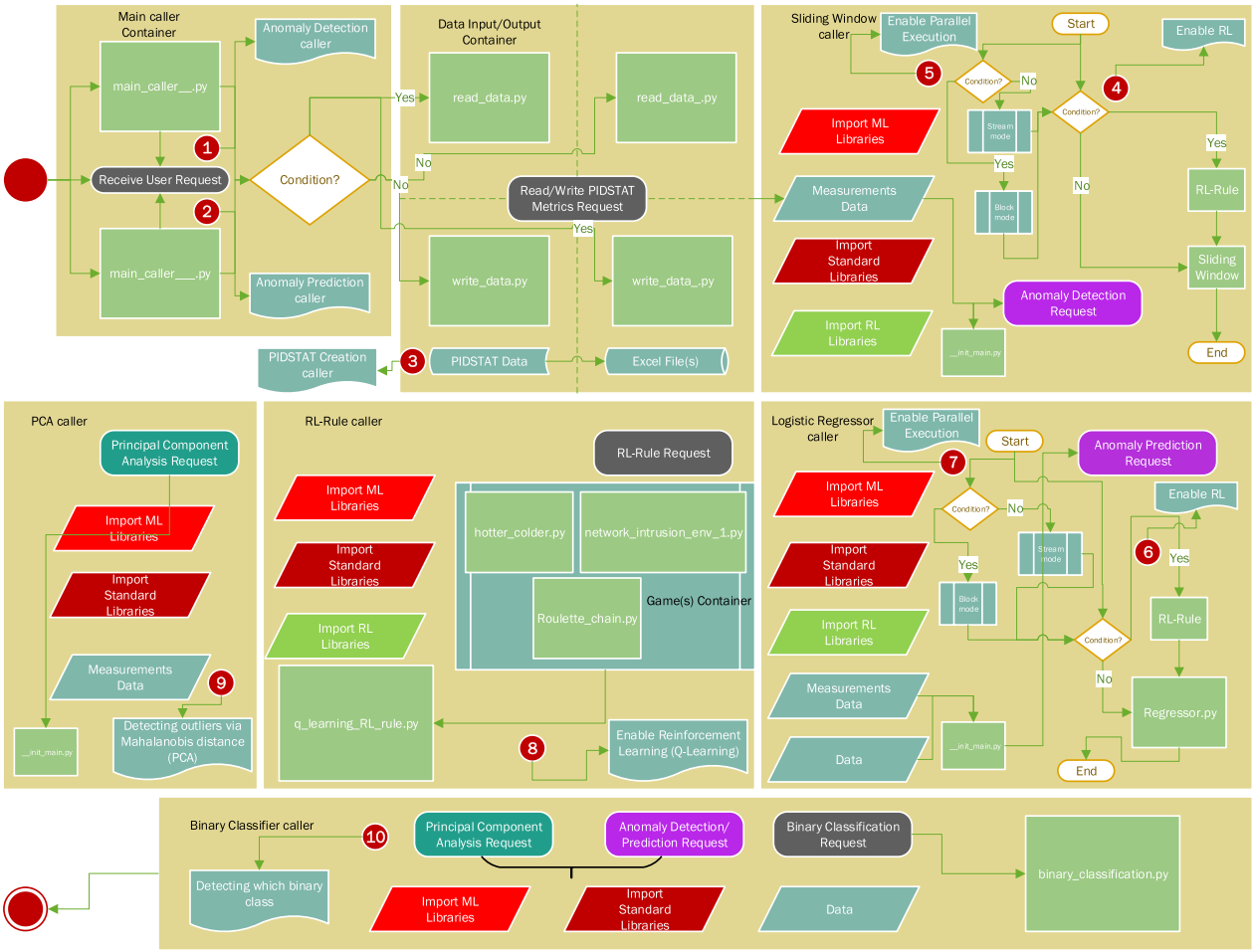


FIGURE 6. Proposed (extended) security framework for IOTA [101].

- The functionality of Principal Component Analysis (PCA) is **optional**.
- The functionality of Binary Classifier EXPECTS bipolar input(s) from {PCA caller} AND {+Sliding Window caller OR +Logistic Regressor caller}.

The framework shown in Figure 6 manages to expand and leverage Figure 5 framework in terms of further protecting Blockchain (DLT)-based IoT (IOTA [101]).

As part of our future work, we will aim to investigate most of these security attacks, such as double-spending compromises against the Tangle, or DDoS attempts to disrupt the availability status of the leading network; by building an attack model with real traffic data, deploying the real attack(s) under a full attack propagation scenario, and proposing a novel secure consensus algorithm, as well as prototyping a security framework as described in Section V.), to enhance security resistance of IOTA with complete evaluations and experimental benchmarking. Based on our ongoing analysis, we conclude that IOTA needs security as outlined in our study and implement the proposed recommendations.

VII. CONCLUSION

In this survey paper, we presented a summary of the most significant and state-of-the-art cybersecurity considerations as well as pitfalls of the typical IOTA implementation. We analyzed the most popular IoT-ledger-based consensus algorithms in terms of security requirements, vulnerabilities as well as attack resistance and also highlighted possible areas of improvement. Notably, the IOTA protocol and its underlying consensus technologies are garnering significant research interest for providing its security. We hope the current research analysis, research work recommendations, future scope, and discussion points will help academics & developers to raise their understanding of the blockchain fundamentals to build better secure consensus designs for secure DLT-IoT integration.

REFERENCES

[1] P. Danzi, A. E. Kalor, C. Stefanovic, and P. Popovski, "Analysis of the communication traffic for blockchain synchronization of IoT devices," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kansas City, MO, USA, May 2018, pp. 1–7, doi: 10.1109/ICC.2018.8422485.

[2] G. Varshney and H. Gupta, "A security framework for IoT devices against wireless threats," in *Proc. 2nd Int. Conf. Telecommun. Netw. (TEL-NET)*, Noida, India, Aug. 2017, pp. 1–6, doi: 10.1109/TEL-NET.2017.8343548.
[3] L. Ghiro, L. Maccari, and R. L. Cigno, "Proof of networking: Can blockchains boost the next generation of distributed networks?" in *Proc. 14th Annu. Conf. Wireless On-Demand Netw. Syst. Services (WONS)*, Isola, France, Feb. 2018, pp. 29–32, doi: 10.23919/WONS.2018.8311658.
[4] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in Internet of Things: Challenges, solutions and future directions," in *Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Koloa, HI, USA, Jan. 2016, pp. 5772–5781, doi: 10.1109/HICSS.2016.714.
[5] A. N. Bikos and N. Sklavos, "The future of privacy and trust on the Internet of Things (IoT) for healthcare: Concepts, challenges, and security threat mitigations," in *Recent Advances in Security, Privacy, and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS)*, K.-C. Li, B. B. Gupta, and D. P. Agrawal, Eds. Boca Raton, FL, USA: CRC Press, 2021.
[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," whitepaper, 2009. [Online]. Available: http://www.bitcoin.org/
[7] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[8] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
[9] S. Roy, M. Ashaduzzaman, M. Hassan, and A. R. Chowdhury, "BlockChain for IoT security and management: Current prospects, challenges and future directions," in *Proc. 5th Int. Conf. Netw., Syst. Secur. (NSysS)*, Dhaka, Bangladesh, Dec. 2018, pp. 1–9, doi: 10.1109/NSysS.2018.8631365.
[10] S. M. Muzammal and R. K. Murugesan, "A study on leveraging blockchain technology for IoT security enhancement," in *Proc. 4th Int. Conf. Adv. Comput., Commun. Autom. (ICACCA)*, Subang Jaya, Malaysia, Oct. 2018, pp. 1–6, doi: 10.1109/ICACCAF.2018.8776806.
[11] S. Yin, J. Bao, Y. Zhang, and X. Huang, "M2M security technology of CPS based on blockchains," *Symmetry*, vol. 9, no. 9, p. 193, Sep. 2017.
[12] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2017, pp. 1–6.
[13] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, Sep. 2018.
[14] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jun. 2017, pp. 468–475.
[15] Q. Bramas, "The stability and the security of the tangle," Univ. Strasbourg, Strasbourg, France, Tech. Rep. hal-01716111, 2018.
[16] S. Popov. (2016). *The Tangle*. [Online]. Available: https://iota.org/
[17] E. Heilman, N. Narula, G. Tanzer, J. Lovejoy, M. Colavita, M. Virza, and T. Dryja, "Cryptanalysis of Curl-P and other attacks on the IOTA cryptocurrency," IACR Cryptol. ePrint Arch., Tech. Rep., 2019/344, Mar. 2019.
[18] G. De Roode, I. Ullah, and P. J. M. Havinga, "How to break IOTA heart by replaying?" in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–7.
[19] L. Tennant, "Improving the anonymity of the IOTA cryptocurrency," Univ. Cambridge, Cambridge, U.K., Tech. Rep. 2017-10-09, Oct. 2017.
[20] B. Baek, "IOTA: A cryptographic perspective," Harvard Univ., Cambridge, MA, USA, Tech. Rep., 2019.
[21] M. Colavita and G. Tanzer, "A cryptanalysis of IOTA's Curl hash function," Harvard College, Cambridge, MA, USA, Tech. Rep., May 2018.
[22] J. Brogan, I. Baskaran, and N. Ramachandran, "Authenticating health activity data using distributed ledger technologies," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 257–266, Jan. 2018, doi: 10.1016/j.csbj.2018.06.004.
[23] A. Cullen, P. Ferraro, C. King, and R. Shorten, "Distributed ledger technology for IoT: Parasite chain attacks," Imperial College London, London, U.K., Tech. Rep., Nov. 2020.
[24] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM J. Comput.*, vol. 17, no. 2, pp. 281–308, Apr. 1988.
[25] (Dec. 8, 2019). *Nash Equilibria*. [Online]. Available: http://hoylab.cornell.edu
[26] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, Jun. 2020.
[27] B. Shabandri and P. Maheshwari, "Enhancing IoT security and privacy using distributed ledgers with IOTA and the tangle," in *Proc. 6th Int. Conf. Signal Process. Integr. Netw. (SPIN)*, Mar. 2019, pp. 1069–1075.
[28] T. Janecko and I. Zelinka, "Impact of security aspects at the IOTA protocol," VŠB-Tech. Univ. Ostrava, Ostrava, Czechia, Tech. Rep., Jan. 2019, vol. 2.
[29] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.
[30] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018.
[31] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.
[32] D. Ding, Q.-L. Han, Y. Xiang, C. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, Jan. 2018.
[33] H. Tschofenig and E. Baccelli, "Cyberphysical security for the masses: A survey of the Internet protocol suite for Internet of Things security," *IEEE Secur. Privacy*, vol. 17, no. 5, pp. 47–57, Sep. 2019.
[34] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things security: A top-down survey," *Comput. Netw.*, vol. 141, pp. 199–221, Aug. 2018.
[35] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017.
[36] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.
[37] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.
[38] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.
[39] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2020.
[40] A. Karakaya and S. Akleylek, "A survey on security threats and authentication approaches in wireless sensor networks," in *Proc. 6th Int. Symp. Digit. Forensic Secur. (ISDFS)*, Mar. 2018, pp. 1–4.
[41] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.
[42] J. Giraldo, E. Sarkar, A. A. Cárdenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber-physical systems: A survey of surveys," *IEEE Design Test*, vol. 34, no. 4, pp. 7–17, Aug. 2017.
[43] A. Algburi, A. Al-Hasnawi, and L. Lilien, "Differentiating security from privacy in Internet of Things: A survey of selected threats and controls," in *Computer and Network Security Essentials*, vol. 6330. Cham, Switzerland: Springer, 2018.
[44] U. Sarfraz, M. Alam, S. Zeadally, and A. Khan, "Privacy aware IOTA ledger: Decentralized mixing and unlinkable IOTA transactions," *Comput. Netw.*, vol. 148, pp. 361–372, Jan. 2019.
[45] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.
[46] S. K. Pinjala and K. M. Sivalingam, "DCACI: A decentralized lightweight capability based access control framework using IOTA for Internet of Things," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, Apr. 2019, pp. 13–18.
[47] G. Bu, W. Hana, and M. Potop-Butucaru, "Metamorphic IOTA," 2019, *arXiv:1907.03628*.
[48] M. A. Brady, I. Ullah, and P. J. M. Havinga, "DOSing distributed ledger technology: IOTA," in *Proc. IEEE 5th Int. Conf. Cryptogr., Secur. Privacy (CSP)*, Jan. 2021, pp. 55–61.
[49] A. Jha, M. Dave, and S. Madan, "Big data security and privacy: A review on issues, challenges and privacy preserving methods," *Int. J. Comput. Appl.*, vol. 177, no. 4, pp. 23–28, Nov. 2017.

[50] P. Charalampidis and A. Fragkiadakis, "When distributed ledger technology meets Internet of Things—Benefits and challenges," 2020, *arXiv:2008.12569*.

[51] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers (DCCL)*, vol. 310, 2016, pp. 4–9.

[52] T. Sharma, S. Satija, and B. Bhushan, "Unifying blockchian and IoT: Security requirements, challenges, applications and future trends," in *Proc. Int. Conf. Comput., Commun., Intell. Syst. (ICCCIS)*, Oct. 2019, pp. 341–346.

[53] *IOTA-VPKI: A DLT-Based and Resource Efficient Vehicular Public Key Infrastructure*. Accessed: Aug. 30, 2018. [Online]. Available: https://autopilot-project.eu/wp-content/uploads/sites/16/2019/07/AS706217643110401154538681524 8_content_1.pdf
[53] => IOTA-VPKI: A DLT-based and Resource Efficient Vehicular Public Key Infrastructure, 27-30 Aug. 2018

[54] A. Tesei, L. Di Mauro, M. Falcitelli, S. Noto, and P. Pagano, "IOTA-VPKI: A DLT-based and resource efficient vehicular public key infrastructure," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Aug. 2018, pp. 1–6.

[55] A. Elsts, E. Mitskas, and G. Oikonomou, "Distributed ledger technology and the Internet of Things: A feasibility study," in *Proc. 1st Workshop Blockchain-Enabled Netw. Sensor Syst.*, Nov. 2018, pp. 7–12.

[56] L. J. W. Vries, "IOTA vulnerability: Large weight attack performed in a network," M.S. thesis, Dept. Elect. Eng., Math. Comput. Sci., Univ. Twente, Enschede, The Netherlands, 2019.

[57] S. Shafeeq, S. Zeadally, M. Alam, and A. Khan, "Curbing address reuse in the IOTA distributed ledger: A cuckoo-filter-based approach," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1244–1255, Nov. 2020.

[58] D. Cai, "A parasite chain attack in IOTA," M.S. thesis, Dept. Elect. Eng., Math. Comput. Sci., Univ. Twente, Enschede, The Netherlands, 2019.

[59] A. Penzkofer, B. Kusmierz, A. Capossele, W. Sanders, and O. Saa, "Parasite chain detection in the IOTA protocol," 2020, *arXiv:2004.13409*.

[60] V. Attias and Q. Bramas, "Tangle analysis for IOTA cryptocurrency," École Normale Supérieure de Rennes-ENS Rennes, Rennes, France, Tech. Rep., Aug. 2018.
[60] École Normale Supérieure de Rennes-ENS Rennes, Rennes, France, August 23, 2018

[61] P. Tedesco and E. Ormancey, "CERN LCG IOTA certification authority certificate policy and certificate practice statement," CERN Eur. Org. Nucl. Res., Meyrin, Switzerland, Tech. Rep. 1.3.6.1.4.1.96.10.7.2.1.1.0, Version 1.0, Revision 1, 2016.

[62] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Appl. Sci.*, vol. 9, no. 9, p. 1788, Apr. 2019.

[63] S.-K. Kim, U.-M. Kim, and J.-H. Huh, "A study on improvement of blockchain application to overcome vulnerability of IoT multiplatform security," *Energies*, vol. 12, no. 3, p. 402, Jan. 2019.

[64] B. Andriamanalimanana, C.-F. Chiang, J. Novillo, S. Sengupta, and A. Tekeoglu, "Parameterized pulsed transaction injection computation model and performance optimizer for IOTA-tango," in *Proc. Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput.* Cham, Switzerland: Springer, 2018, pp. 74–84.

[65] K. R. Özyilmaz and A. Yurdakul, "Work-in-progress: Integrating low-power IoT devices to a blockchain-based infrastructure," in *Proc. Int. Conf. Embedded Softw. (EMSOFT)*, 2017, pp. 1–2.

[66] Y. Li, B. Cao, M. Peng, L. Zhang, L. Zhang, D. Feng, and J. Yu, "Direct acyclic graph based ledger for Internet of Things: Performance and security analysis," 2019, *arXiv:1905.10925*.

[67] S. Paavolainen and P. Nikander, "Security and privacy challenges and potential solutions for DLT based IoT systems," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2018, pp. 1–6.

[68] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable Blockchain for IoT security and anonymity," *J. Parallel Distrib. Comput.*, vol. 134, pp. 180–197, Dec. 2019.

[69] U. Sinha, A. A. Hadi, T. Faika, and T. Kim, "Blockchain-based communication and data security framework for IoT-enabled micro solar inverters," in *Proc. IEEE CyberPELS (CyberPELS)*, Apr. 2019, pp. 1–5.

[70] G. Bu, Ö. Gürcan, and M. Potop-Butucaru, "G-IOTA: Fair and confidence aware tangle," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Paris, France, Apr. 2019, pp. 644–649, doi: 10.1109/INFCOMW.2019.8845163.

[71] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[72] V. Buterin. (2013). *Ethereum White Paper*. Accessed: Apr. 2, 2018. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[73] E. Androulaki *et al.*, "Hyperledger fabric: A distributed operating system for permissioned blockchains," 2018, *arXiv:1801.10228*.

[74] (2011). *Litecoin*. Accessed: Feb. 4, 2018. [Online]. Available: https://litecoin.org/

[75] (2016). *Quorum Whitepaper*. Accessed: Feb. 1, 2018. [Online]. Available: https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum%20Whitepaper%20v0.1.pdf

[76] (2017). *HDAC*. Accessed: Feb. 1, 2018. [Online]. Available: https://hdac.io/

[77] I. A. Naidu. (2017). *Nestle, Unilever, Tyson and Others Team With IBM on Blockchain, Reuters*, Accessed: Oct. 20, 2017. [Online]. Available: http://www.reuters.com/article/us-ibm-retailers-blockchain/nestle-unilever-tyson-and-others-team-with-ibm-on-blockchain-idUSKCN1B21B1

[78] M. Samaniego and R. Deters, "Internet of smart things—IoST: Using blockchain and CLIPS to make things autonomous," in *Proc. IEEE Int. Conf. Cognit. Comput. (ICCC)*, Honolulu, HI, USA, Jun. 2017, pp. 9–16.

[79] (2017). *The Lisk Protocol*. Accessed: Feb. 1, 2018. [Online]. Available: https://docs.lisk.io/docs/the-liskprotocol

[80] R. C. Merkle, "A certified digital signature," in *Proc. Conf. Theory Appl. Cryptol.* Lyon, France: Springer, 1989, pp. 218–238.

[81] E. Heilman. (Sep. 7, 2017). *IOTA Vulnerability Report: Cryptanalysis of the Curl Hash Function Enabling Practical Signature Forgery Attacks on the IOTA Cryptocurrency*. [Online]. Available: https://github.com/mitdci/tangled-curl/blob/master/vuln-iota.md

[82] S. A. P. Kumar, B. Bhargava, R. Macedo, and G. Mani, "Securing IoT-based cyber-physical human systems against collaborative attacks," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Jun. 2017, pp. 9–16.

[83] D. Eastman and S. A. P. Kumar, "A simulation study to detect attacks on Internet of Things," in *Proc. IEEE 15th Int. Conf Dependable, Autonomic Secure Comput. (DASC/PiCom/DataCom/CyberSciTech)*, Nov. 2017, pp. 645–650.

[84] H. Malviya. (2016). *How Blockchain Will Defend IoT*. Accessed: Feb. 1, 2018. [Online]. Available: https://ssrn.com/abstract=2883711

[85] P. Veena, S. Panikkar, S. Nair, and P. Brody, "Empowering the edge-practical insights on a decentralized Internet of Things," in *Empowering the Edge-Practical Insights on a Decentralized Internet of Things*, vol. 17. Armonk, NY, USA: IBM, 2015.

[86] S. Gan, "An IoT simulator in NS3 and a key-based authentication architecture for IoT devices using blockchain," M.S. thesis, Indian Inst. Technol. Kanpur, Kanpur, India, Tech. Rep., Jul. 2017.

[87] (2017). *Chain of Things*. Accessed: Feb. 1, 2018. [Online]. Available: https://www.blockchainofthings.com/

[88] (2017). *Filament*. [Online]. Available: https://filament.com/. (Accessed 1, Feb. 2018).

[89] (2017). *Modum*. Accessed: Feb. 1, 2018. [Online]. Available: https://modum.io/

[90] S. G. Prisco. (2016). *It to Introduce Smart Locks Linked to Smart Ethereum Contracts, Decentralize the Sharing Economy*. Accessed: Feb. 1, 2018. [Online]. Available: https://bitcoinmagazine.com/articles/slock-it-to-introduce-smart-locks-linked-to-smart-ethereum-contracts-decentralize-the-sharing-economy-1446746719/

[91] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[92] (2017). *LO3ENERGY*. Accessed: Feb. 1, 2018. [Online]. Available: https://lo3energy.com/

[93] (2017). *Aigang*. Accessed: Feb. 1, 2018. [Online]. Available: https://aigang.network/

[94] (2017). *My Bit*. Accessed: Feb. 1, 2018. [Online]. Available: https://mybit.io/

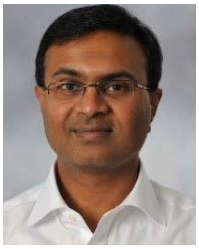
[95] M. Samaniego and R. Deters, "Hosting virtual IoT resources on edge-hosts with blockchain," in *Proc. IEEE Int. Conf. Comput. Inf. Technol. (CIT)*, Yanuca, Fiji, Dec. 2016, pp. 116–119.

[96] M. Aazam and E.-N. Huh, "Fog computing and smart gateway based communication for cloud of things," in *Proc. 2nd Int. Conf. Future Internet Things Cloud*, Barcelona, Spain, Aug. 2014, pp. 27–29.

[97] (2017). *Ethembedded*. Accessed: Feb. 1, 2018. [Online]. Available: http://ethembedded.com/

[98] (2017). *Raspnode*. Accessed: Feb. 1, 2018. [Online]. Available: http://raspnode.com/
[99] K. Wüst and A. Gervais, "Do you need a blockchain?" IACR Cryptol. EPrint Arch., Tech. Rep. 2017/375, Apr. 2017.
[100] (2017). *Ethraspbian*. Accessed: Feb. 1, 2018. [Online]. Available: http://ethraspbian.com/
[101] A. N. Bikos and S. Kumar, "Reinforcement learning-based anomaly detection for Internet of Things distributed ledger technology," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Athens, Greece, Sep. 2021, pp. 1–7.
[102] *European Blockchain Pre-Commercial Procurement*. Accessed: Oct. 2, 2021. [Online]. Available: https://blog.iota.org/phase-2-eu-blockchain-pre-commercial-procurement/
[103] B. Bhushan, P. Sinha, K. M. Sagayam, and J. A. Onesimu, "Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions," *Comput. Electr. Eng.*, vol. 90, Mar. 2021, Art. no. 106897.
[104] M. Bhandary, M. Parmar, and D. Ambawade, "A blockchain solution based on directed acyclic graph for IoT data security using IoTA tangle," in *Proc. 5th Int. Conf. Commun. Electron. Syst. (ICCES)*, Jun. 2020, pp. 827–832.
[105] F. Ghaffari, E. Bertin, J. Hatin, and N. Crespi, "Authentication and access control based on distributed ledger technology: A survey," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 79–86.
[106] I. Ullah, G. de Roode, N. Meratnia, and P. Havinga, "Threat modeling—How to visualize attacks on IOTA?" *Sensors*, vol. 21, no. 5, p. 1834, Mar. 2021.
[107] M. Alshaikhli, T. Elfouly, O. Elharrouss, A. Mohamed, and N. Ottakath, "Evolution of Internet of Things from blockchain to IOTA: A survey," *IEEE Access*, vol. 10, pp. 844–866, 2022.
[108] N. Gupta, "Security and privacy issues of blockchain technology," Stud. Big Data, Manav Rachna Int. Inst. Res. Stud., Faridabad, India, Tech. Rep., Sep. 2019, vol. 60.
[109] A. M. Mohideen and S. G. Kumar, "Privacy challenges and enhanced protection in blockchain using erasable ledger mechanism," in *Expert Clouds and Applications*. Singapore: Springer, 2021.
[110] A. Islam, A. A. Amin, and S. Y. Shin, "FBI: A federated learning-based blockchain-embedded data accumulation scheme using drones for Internet of Things," *IEEE Wireless Commun. Lett.*, early access, Feb. 16, 2022, doi: 10.1109/LWC.2022.3151873.
[111] A. Islam, T. Rahim, M. Masuduzzaman, and S. Y. Shin, "A blockchain-based artificial intelligence-empowered contagious pandemic situation supervision scheme using Internet of Drone Things," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 166–173, Aug. 2021.
[112] C. Fan, "Performance analysis and design of an IoT-friendly DAG-based distributed ledger system," Univ. Alberta, Univ. Edmonton, Edmonton, AB, Canada, Tech. Rep., 2019.
[113] C.-T. Li, C.-C. Lee, C.-Y. Weng, and C.-M. Chen, "Towards secure authenticating of cache in the reader for RFID-based IoT systems," *Peer-to-Peer Netw. Appl.*, vol. 11, no. 1, pp. 198–208, Jan. 2018.

ANASTASIOS N. BIKOS graduated from the Department of Computer Engineering and Informatics, School of Engineering, University of Patras, Greece, in 2015. He received the B.S. and M.S. degrees in computer engineering and informatics. His research interests include artificial intelligence, digital satellite communications, FPGA, signal processing, information security, system-on-a-chip (SoC) security systems, 5G/6G, and IoT security and hardware security. The results of his research have been published in technical literature. He has participated in research and development activities in the areas of his study extensively over recent years. He is keen and passionate to perform high-quality research and always adapts the "architecture," not only "engineering" approach into problem-solving, no matter how complicated problems seem to be.



SATHISH A. P. KUMAR (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from the University of Louisville, Louisville, KY, USA, in 2007. He is currently an Associate Professor of computer science with the Department of Electrical Engineering and Computer Science, Cleveland State University, Cleveland, OH, USA. He is the Co-Director of Cleveland State University TECH Hub, an interdisciplinary center related to technology. He is directing Intelligent Secure Cyber-Systems Analytics and Applications Research (ISCAR) Laboratory, Cleveland State University. He has published more than 70 technical papers in international journals and conference proceedings. His current research interests include cybersecurity, machine learning, big data analytics, and secure distributed systems and their applications.