 doi:10.20944/preprints202208.0115.v1

Article

Internet of Things Aware Secure Dew Computing Architecture for Distributed Hotspot Network: A Conceptual Study

Partha Pratim Ray[1,*] and Karolj Skala[2]

[1] Department of Computer Applications, Sikkim University, Gangtok, India; parthapratim-ray1986@gmail.com
[2] Center for Informatics and Computing Science, Ruđer Bošković Institute, Zagreb, Croatia; skala@irb.hr
* Correspondence: parthapratimray1986@gmail.com, skala@irb.hr

Abstract: Building a widely distributed hotspot network is a very tedious task due to its complexity. Providing security, fully distributed network services, and cost-conscious impact are the major challenges behind this goal. To overcome these issues, we have presented a novel distributed hotspot network architecture with five layers that can provide large-scale hotspot coverage as an assimilated result. Our contributions to this new architecture highlight important aspects. First, scalability can be increased by including many Internet-of-Things (IoT) devices with sensors and Wi-Fi and/or LoraWAN connectivity modules. Second, hotspot owners can rent out their hotspots to create a distributed hotspot network in which the hotspots can act as an ordinary data gateway, a full-fledged hotspot miner, and a lightweight hotspot miner to earn crypto tokens as rewards for certain activities. Third, the advantages of Wi-Fi and LoraWAN can be seamlessly leveraged to achieve optimal coverage, higher network security, and suitable data transmission rate for transferring sensor data from IoT devices to remote application servers and users. Fourth, blockchain is used to enhance the decentralized behavior of the architecture presented here by providing immutability and independence from a centralized regulator and making the network architecture more reliable and transparent. The main feature of our paper is the use of the tau-computing paradigm along with hotspots to improve availability, Internet backhaul-agnostic network coverage, and synchronous update capability, and tau-aware leasing to strengthen and improve coverage. We also discuss the key challenges and future roadmap that require further investment and deployment.

Keywords: Dew computing; Internet of Things; Blockchain; Hotspot Network

1. Introduction

The world has witnessed several technological advances, especially in the areas of pervasive computing, ubiquitous computing, security, and open source hardware (OSH) development [1-3]. Since its inception, IoT has experienced tremendous growth in all application areas such as agriculture, industry, automation, smart city, and healthcare [4-7]. Every time an IoT device collects sensor data from a physical entity, it requires a gateway or Internet connection to transmit this data to the remote applications and users. This results in huge network traffic and degradation of the network's backhaul dependency. Apart from this, the extensive use of IoT sensor data for transmission over long distances incurs costs and is associated with significant power consumption [8-10]. In the absence of a suitable network technology, IoT sensor data might be limited to the near periphery from which it originates. As a result, quality of service is minimized and reliability is neglected. As a result, the entire IoT ecosystem evolves into an unstable concept where IoT sensor data is not always available to remote applications. Existing Internet backhaul and cloud computing-centric approaches are mainly responsible for such obstacles.

Standalone hotspots are regularly used in our daily life [11][12]. Normally, a cell phone with subscriber network connectivity and available data packets can be seamlessly used

 doi:10.20944/preprints202208.0115.v1

as a mobile hotspot for other interested devices nearby to access the Internet. It becomes problematic when the hotspot that an interested user's device is trying to connect to has no network coverage or is out of subscription, limiting the ability to break the coverage of the hotspot for the interested device [13][14]. This calls into question the usability, quality of service, and reliability of such hotspots.

Dew computing is a recent development in computing that aims to leverage in-network dependencies and collaborative approaches for remote cloud servers [15-17]. Dew servers are such devices that follow the dew computing idea and perform needed activities such as data access to local machines independent of network availability [18]. Dew computing is based on the principles of synchronization function, which allows such Dew devices to operate locally and require very little Internet connection to synchronize with their cloud replica [19-21]. In Dew computing, each user has a cloud replica with a local clone of the same content. At the time of writing, dew computing is still in its early stages and thus focuses mainly on services related to network data access for its end devices [22]. However, the long-term goal of dew computing is to provide higher reliability, better availability, and user-centric data access, as well as a provider that is primarily independent of Internet connectivity.

Distributed hotspot networks are an idea that has been discussed for a long time and has received increasing attention in both industry and academia in recent years. However, to date, no such fully self-organizing distributed hotspot network exists, either in research or in practice [23]. The idea of using Wi-Fi as an enabler for hotspot deployment is currently under investigation [24]. However, Wi-Fi struggles with limited range, signal interference, bandwidth usage, and security [25]. Using Wi-Fi on a large number of IoT devices may pose various challenges in terms of power consumption, which may shorten the battery life of IoT devices [26]. On the other hand, LoraWAN can be considered as an alternative to Wi-Fi to provide wide area connectivity with improved security and battery life of IoT devices [26][27]. However, it faces problems such as low data rate, small packet size, and unsuitability for real-time applications. In addition, it is believed that a person who wants to provide their hotspot as a gateway for IoT devices may face paid subscriptions, which may prevent them from providing their hotspot device to an unknown IoT device. When an IoT device wants to connect to the hotspot of an unknown person in its nearby coverage area, authentication and security become the most important factors. Security and authentication issues can be solved by incorporating blockchain and appropriate crypto tokens as incentives for hotspot owners. Blockchain is an immutable decentralized technology that aims to provide inherent security for the stored data and access by nodes (miners and validators) with or without authorization [28][29]. In this way, a complete business model can be formulated where a distributed hotspot network can be developed that operates in a fully decentralized manner and offers incentives to hotspot owners to rent out their hotspots to serve IoT devices in the vicinity [30-32].

In this paper, we present a novel idea for an IoT-based secure distributed hotspot network to solve the existing problems in creating and deploying a hotspot network that has the potential to succeed as a business model. The main contributions of this work can be summarized as follows:

- Using IoT devices as sensor data generators under the supervision of nearby hotspots that may be unknown to these IoT devices.
- The architecture presented here is a distributed hotspot architecture that can be assimilated with many IoT devices to scale the data generation process.
- The presented architecture can leverage highly secure and authenticated hotspot network coverage by using blockchain.
- The whole concept behind the architecture is to use a decentralized approach for the connected hotspot devices that can act as distributed gateways.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 August 2022 doi:10.20944/preprints202208.0115.v1

- Such hotspots can earn crypto tokens as rewards for certain activities such as data transmission, coverage stability, validation and mining.
- Authentication and security-enabled hotspot networks can span several miles without requiring existing cellular networks.
- Dew computing is integrated into hotspot devices to provide increased computing power and capacity independent of Internet backhaul.
- By deploying Dew servers in the hotspots, they can be configured to become full-fledged, lightweight, data-only hotspots.
- The hotspots presented here can perform mining, validation, IoT data coverage, and crypto token collection from the blockchain.
- Remote users and application servers can be connected to such secure, authentication-enabled incentive hotspot networks, through which distributed IoT devices can transmit sensor data over long distances.
- In this design, IoT devices can be equipped with Wi-Fi and/or LoraWAN antenna modules that can be reasonably deployed according to data transmission needs (low or high) and distance requirements.
- The presented architecture can open a new business model where hotspot owners can earn crypto tokens from their hotspots to reduce subscription and operational costs and make the whole network ecosystem sustainable.

The concept paper is organized as follows. Section 2 discusses related work. Section 3 presents the background idea on various technologies used to develop a secure and distributed hotspot network. Section 3 provides a detailed description of the novel architecture. Section 4 concludes this paper with a discussion, important challenges, future work, and a conclusion.

2. Related Work

We perform an extensive literature search to find related work relevant to our work. We searched IEEE Xplore and Google Scholar to find most of the related articles in this section. We note that none of the works relate to the tau computing paradigm for solving the new dimensions of distributed hotspot network formation. The majority of the articles don't consider IoT devices as part of their models. None of the articles discuss the integration of LoraWAN into the hotspot network. For example, Zha et al [33] discuss blockchain-based energy distribution with detailed policies, but lack a detailed process for forming a distributed hotspot network. Zhao et al [34] don't address hotspot aspects in the design of blockchain-based distributed networks. Messié et al [35] use blockchain with hotspots to build the BALAdIN framework for multi-actor access network formation without providing clear guidance for de-signing distributed hotspot networks.

Table 1. Comparative analysis of related works.

Paper	Blockchain	IoT	Hotspot	Wi-Fi	LoraWAN	Dew Computing	Key Contributions	Limitations
Zha et al. [33]	Yes	No	Yes	Partial	Partial	No	Blockchain aware energy, review, policy recommendations, applications	Lacks hotspot network design approach
Zhao et al. [34]	Yes	Partial	No	No	No	No	Blockchain distributed network design aspects, traceable, tamper-proof design	Hotspot discussion is minimal
Messié et al. [35]	Yes	No	Yes	Partial	No	No	BALAdIN framework, multi-actor access network,	No clear direction on distributed hotspot

 doi:10.20944/preprints202208.0115.v1

Lopez et al. [36]	Yes	No	No	Partial	No	No	Choice modeling, federated learning, distributed privacy-aware design	No analysis about distributed model is made
Janiesch et al. [37]	Yes	No	Yes	Yes	No	No	Wi-Fi sharing architecture, payment channel networking, evaluation of architecture	Distributed behavior not analyzed
Yang et al. [38]	Yes	No	Partial	Partial	No	No	Pricing mode, wireless caching reward, cache quality, cache content dispersion	Hotspot distributed network not covered
Zhao et al. [39]	Yes	No	Partial	No	No	No	Energy transaction, multi-microgrid, energy trading	Hotspot aware design lacks
Kim et al. [40]	Yes	No	Partial	Yes	No	No	Wi-Fi security model, secure models using smart contracts to safeguard Wi-Fi vulnerability	Distributed hotspot discussion missing
Ivanov et al. [41]	Yes	Partial	Yes	Yes	No	No	SmartWiFi architecture, Hansa handshake/service, smart contract, payment, refunds, security analysis	Hotspot distributed-ness lacks
Pustišek et al. [42]	Yes	Yes	Yes	Yes	No	No	Low-bandwidth distributed applications framework (LDAF) architecture, distributed model	Consensus algorithm no specified, no scalability
Ma et al. [43]	No	No	Yes	Yes	No	No	Security risk analysis, android data cloning, evaluation	No blockchain involved
Our Model	Yes	Yes	Yes	Yes	Yes	Yes	Distributed hotspot architecture design, blockchain aware secure IoT device data transmission, dew computing inclusion, scalable, incentive	Implementation needed

Lopez et al. [36] discusses about choice-based modeling of distributed network on top of the federated learning, but way is paved for distributed nature of hotspots. Janiesch et al. [37] shows a Wi-Fi sharing architecture with payment channel formation, but doesn't show distributed behavior of the underlying hotspots. Yang et al. [38] uses pricing mode for paving the wireless caching reward with cache content dispersion mechanism. Zhao et al. [39] shows energy transaction mechanism with energy trading facility, however no study is performed for hotspot distributed network creation. Kim et al. [40] presents Wi-Fi security model by using smart contract to safeguard from Wi-Fi vulnerability. Ivanov et al. [41] designs a smartWiFi architecture by using Hansa handshaking procedure and performs payments via crypto-token. However, it is quite on dew computing aspects. Pustišek et al. [42] presents a low-bandwidth distributed application framework where LoraWAN aware inclusion scheme is not discussed. Ma et al. [43] performs security analysis on top of Android data cloning where evaluation is paved without involving the blockchain.

Our Key Contributions

 doi:10.20944/preprints202208.0115.v1

Our contributions are new with respect to the related works presented in this section as follows.

- We use dew computing paradigm that can provide independence on the integrated hotspot nodes. Doing so, our architecture can work in rental basis where actual hotspot network can be formed in purely distributed manner. Dew computing uses high reliable synchronization techniques that helps the connected devices to use the network even when a given dew system is not able to process the connected device's request. Dew computing can form *dewlets* that supports rental facility of network coverage from nearby hotspots to enrich availability and overall quality of service.
- Dew server-based hotspots can act as miner and validators to pave reliability factor of the blockchain network. Based on PoC challenge, once a hotspot miner or validator solves the challenge, can establish the reliability is established. The hotspot miner upon completion of certain PoC and data transmission activities can earn crypto-token which can be reflected in the wallets of the respective hotspot owners.
- Our architecture uses IoT-based devices as the data collecting nodes that are able to send the data to remote application servers or users to facilitate visualization, monitoring or related tasks. Millions of IoT devices can be integrated with the presented architecture to improve scalability.
- Our architecture is able to cope up with standard IEEE 802.1X authentication which works on top of IEEE 802.11u standard. This ensures secure and more effective authentication process.

3. Background

In this section, we discuss about IoT, dew computing, blockchain and hotspot technologies to under how they work and existing issues.

3.1. Internet of Thing (IoT)

IoT describes a set of physical or digital objects that communicate via the Internet or similar communication technologies [44-46]. Such objects are referred to as "things", which are usually equipped with sensors, actuators, processing power, memory, and software to perform the required tasks [47-49]. The applications of IoT are very diverse and range from smart heating, smart agriculture, smart automation, smart military, smart industry, smart city, smart horticulture, smart building, smart consumer applications, smart health monitoring, and smart supply chain management [50-51]. As the number of IoT devices is rapidly increasing, several governmental and international agencies are involved in developing policies, regulatory guidelines, and related standards [52].

IoT ecosystems are enabled by various communication and networking technologies: (i) short-range: e.g., Bluetooth, near-field communication, Wi-Fi, Z-Wave, radio frequency identification (RFID), (ii) medium-range: e.g., ZigBee, LTE-advanced, and (iii) long-range: e.g., cellular, satellite communication, and low-power wide-area networks. Wired alternatives such as Ethernet, fiber, and powerline communications (PLC) can be complemented with existing IoT infrastructure [53-54]. The IoT also supports heterogeneity and addressability. Despite the tremendous prospects, IoT suffers from the problem of platform fragmentation, privacy, autonomy, data storage, security, design, environmental impact, and control mechanisms.

 doi:10.20944/preprints202208.0115.v1

3.2. Blockchain

A blockchain refers to a growing list of blocks that are cryptographically linked together. Typically, a block consists of transaction data (in the form of a Merkle tree), block height, timestamp, cryptographic hash of the associated block, and nonce [55]. Other key components such as the threshold signature of an existing consensus group may be included in each of the blocks. Blockchains are managed by a peer-to-peer network, and typically each node of the blockchain contains a distributed ledger [56]. These nodes adhere to the same network protocol for communicating with other nodes in the blockchain and for validating new blocks. Blockchains are inherently immutable and decentralized and have very high fault tolerance [57-58]. Mining is the most important task of a blockchain. In general, a mining node can solve a puzzle (mathematical problem) to get a chance to add a new block as the next block to the blockchain. Thus, a miner can earn crypto tokens as a reward. He can also get a certain amount from the transaction fee for all transactions in that block [59]. The main goal of a mining node is to ensure the reliability of the work performed on the blockchain network by using a consensual protocol such as Proof of Work (PoW) and Proof of Stake (PoS) [60]. The mining process can be performed in the form of a pool of miners, and in pool mining, the chance of crypto reward is higher than in single mining. On the other hand, the validation task is performed by a validator node in the blockchain network, which is involved in disseminating messages to almost all nodes. Sometimes, the validators can take over the mining task seamlessly [61]. Usually, an epoch is set in which a certain group of validators is selected to act as a consensus group. At the end of each epoch, a new group of validators is selected to act as a new consensus group for validating new blocks. Generally, rewards are distributed per block or per epoch via a specific reward transaction. Various types of transactions are possible in a blockchain, some of which are: Gateway addition, location confirmation, chain variable, data credit, multiple payment, rotation, consensus algorithm execution, opening or closing state channels, and security exchange [62-63].

There are four types of blockchains: (i) public: here there are no access restrictions, a node following a standard blockchain communication protocol can act as a validator and send transactions to other such nodes with Internet connectivity, (ii) private: (iii) hybrid: This is a combination of public and private blockchain functions, and (iv) sidechains: this is an independent blockchain that can run in parallel with the main blockchain by connecting sidechains in both directions and communicating with the main blockchain [64-65]. Major applications of blockchain include cryptocurrencies, smart contracts, financial services, online games, supply chain management, domain names, and voting. Blockchains can interact with other blockchain systems to transfer digital assets.

3.3. Dew Computing

Dew Computing provides a new way for end users (Dew users) to connect to cloud-based content without relying on Internet backhaul [66]. It enables an exciting idea where a Tau user can access cloud-based data using their own Tau device without requiring minimal intervention in the Internet connection. Tau users can access the same content as a local copy of the cloud content [67-68]. Once the Internet connection is restored, changes are homogenized between the local and cloud content. This minimizes the dependency on the cloud, where an end user needs an Internet connection every time he wants to access the cloud data. Actually, dew computing aims to solve the problems of offline access to data in the existing cloud computing paradigm [69]. Traditional cloud content and configurations are far from user self-control, as such services are provided exclusively at the enterprise level. Dew computing enables users to match endpoint capabilities with cloud services in a more reliable approach [70-72]. It

 doi:10.20944/preprints202208.0115.v1

depends on two aspects: (i) independence: a local Tau device can operate independently of cloud services, and (ii) collaboration: a local Tau device can communicate with cloud services when Internet connectivity is available or synchronization is desired. A Tau virtual machine (DVM) is required on the user's Tau device, which can take the help of a Tau server, a data analytics server, and a Tau device decision-making approach [73]. Tau computing can provide multiple services that are equivalent to cloud computing, such as data in Tau, platform in Tau, data in Tau, infrastructure in Tau, web in Tau, software in Tau, storage in Tau, and database in Tau [74].

The main advantages of Tau computing over Cloud, Fog, or Edge computing paradigms can be summarized as follows: (i) negligible latency, (ii) negligible jitetring effects, (iii) highly location-aware behavior, (iv) highly distributed geolocated services, (v) very low probability of data redirection attacks, (vi) targets mobile users, (vii) requires limited resources or hardware capacity, (viii) very high user experience, (ix) very low Internet dependency, (x) high delay tolerance, and (xi) very high computing power [75-76].

The dew computing paradigm is seen as an extension of the cloud computing scenario, but at the extreme edge of the network where end users can directly access the Internet [77]. It follows a strict computing hierarchy when it cannot provide the required services to the end users. A tau image for the user-owned cloud repository can be used in the user-owned tau system [78]. Therefore, synchronization plays an important role in Dew computing. Process synchronization with timestamp can be very useful for Dew computing users. The functions of data replication and distribution-oriented transparency can be easily complemented by Internet access to Dew computing data. In case of local data loss, there is a great chance to recover the same data from the cloud storage. In addition, rule-based data collection, scalability, and high reliability are important aspects of Tau computing that provide a minimalist approach to Internet backhaul, so that the user experience can be greatly improved [79]. Tau data rental services can be offered between Tau devices in close proximity, allowing a Tau user to access Internet data even if their personal Internet data is unavailable or restricted for some reason. In this way, Tau computing can serve as a hotspot network entity.

3.4. Hotspot

In general, a hotspot is a physical location where users can access the Internet. Typically, Wi-Fi technology is used to connect a Wi-Fi router that is connected to an Internet service provider (ISP) via Ethernet or a wireless local area network (WLAN). Hotspots can be both public and private [80-82]. Public hotspots are established and maintained by businesses or government agencies for use by the public, especially at bus stops, train stations, libraries, hospitals, supermarkets, and university buildings. Private hotspots are usually set up in hotels, restaurants or cafés. Public hotspots are usually served by wireless access points (WAPs) configured for Internet access. These WAPs are controlled and managed by local authorities. A facility that has broadband or fibre Internet access can provide wireless Internet access through the WAPs [83-85]. These WAPs are connected to routers or gateways that provide seamless Internet connectivity.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 August 2022 doi:10.20944/preprints202208.0115.v1

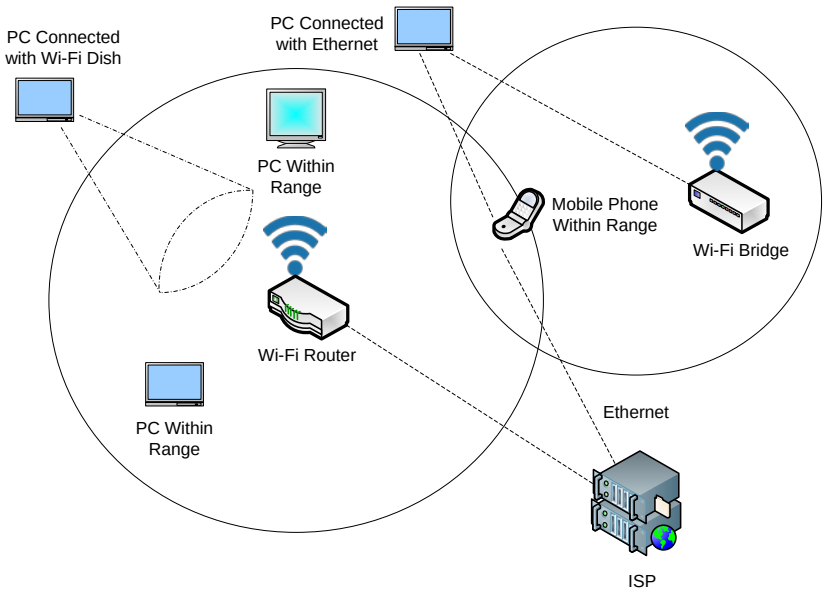

Figure 1. Generic structure of Wi-Fi hotspots.

3.4.1. Tethering

A private hotspot can be created, configured, and managed using tethering. Tethering uses a phone as a modem (PAM) that shares the phone's (device's) Internet connection with authorized (by password or pin number) nearby devices such as computers, smartphones, tablets, and notebooks. The connection in tethering is established via a physical cable connection (e.g. a USB cable), Bluetooth or WLAN-based Wi-Fi technologies. Nowadays, tethering is done via WLAN, which is called a mobile hotspot. Such mobile hotspots can serve as both dynamic and portable routers for Internet access. Most operating systems for mobile devices (Windows 6.5 or higher, Android 2.2 or higher, iOS 3.0 or higher) support this feature. These smart devices are equipped with the necessary software and hardware to enable wireless Internet access [86-87]. Tethering over Wi-Fi is also referred to as a personal hotspot. Tethering can also be done via Network Address Translation (NAT) based on the existing Internet connection of the mobile device. Such NAT is used for IPv4 networks where the mobile device has a single IPv4 address, but multiple devices can be identified with such a network address.

3.4.2. Hotspot Varieties

Hotspots may be operated in open public network space as free or closed public networks with a central hotspot management system operated by a local authority. Hotspots can be operated commercially, requiring users to authenticate or pay before using Internet data [88]. Software-enabled access points (SoftAP) are one such type of hotspots that can be used in a computer or cell phone to turn it into a virtual router. SoftAP can be used to configure Wi-Fi enabled devices (e.g., IoT devices) that do not have a display or other inputs. There are two major challenges in doing so: (i) manually connecting to the SoftAP network, and (ii) if lost or given the wrong passkey, the disconnected device is almost irretrievably lost for further use of the SoftAP network.

3.4.3 Hotspot 2.0

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 August 2022 doi:10.20944/preprints202208.0115.v1

Hotspot 2.0 is also known as Passpoint (Wi-Fi certified), which can be used to access Wi-Fi and Wi-Fi Alliance. The purpose of Hotspot 2.0 is to allow the Wi-Fi enabled mobile device to automatically connect to a Wi-Fi subscriber when the mobile devices move into the Hotspot 2.0 region [89-90]. In this way, a better on-demand service is provided to the mobile devices. In addition, a scenario for better bandwidth utilization can be developed, where the load on the network operator's infrastructure is reduced to minimize network traffic. Hotspot 2.0 is based on the IEEE 802.11u standard to enable cellular-like roaming. A mobile device supported by IEEE 802.11u and subscribed to Hotspot 2.0 can automatically join the network and roam accordingly [91-93]. A dynamic fairness model is used to charge for the use of the Internet connection in this context. A user priority list is recommended to charge for Internet usage based on time criticality and network traffic types (audio, video, data). Hotspot 2.0 is deployed based on the IEEE 802.11u standard, which defines a formulation for a terminal device to receive WLAN-related information. Hotspot 2.0 consists of some key elements, such as (i) a terminal device (STA) that supports WPA2, Hotspot 2.0, 802.1X and Access Network Query Protocol (ANQP), (ii) an access point (AP): the Hotspot 2.0, supports WPA2-801.1X and acts as an ANQP server, it can send Hotspot 2.0 network information to the connected STAs, (iii) an access controller (AC): that supports 802.1X configuration between the Aps in stacks, (iv) AAA server: it supports various encryptions such as Extensible Authentication Protocol (EAP) authentication and key agreement (AKA)/subscriber identification module (SIM), Transport Layer Security (LTS), Tunneled Transport Layer Security (TTLS), it can also obtain authentication vectors from the Home Location Register (HLR), and (vi) BOSS: It provides important operational support as an end-to-end business provider to perform regular customer-facing tasks such as billing, rating, and general service [94].

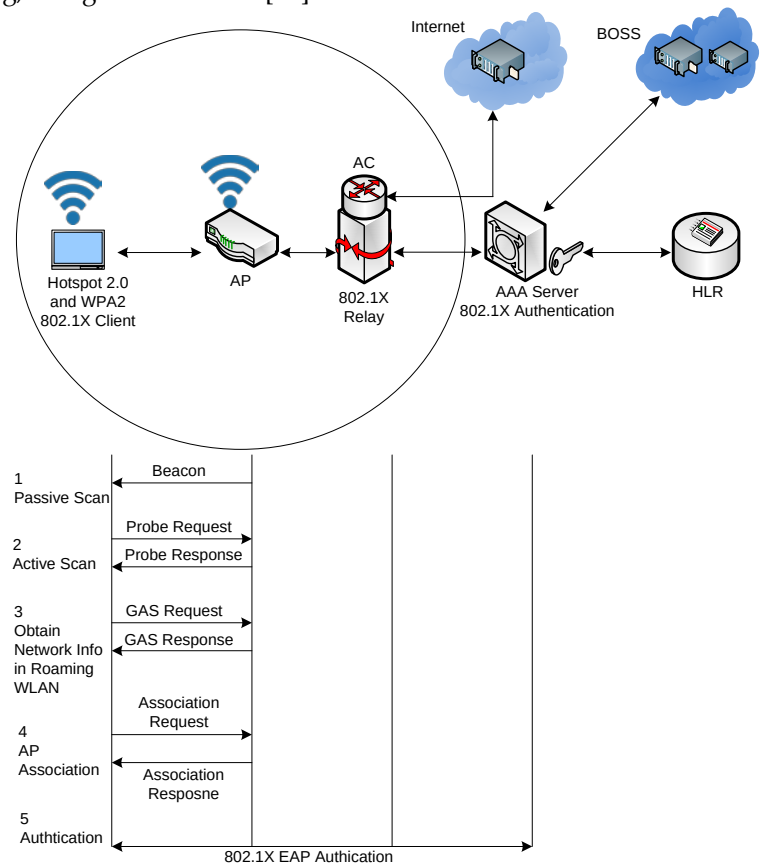

Figure 2. Generic structure of hotspot 2.0.

 doi:10.20944/preprints202208.0115.v1

Network discovery and selection is an important job of hotspot 2.0. It is formulated as follows. The network discovery service needs the packet exchange between end STA module and the access point. End STA module can perform active and passive scan. Both scans can take place parallelly. The STA device must have pre-registration with home network with pre-configured network cards, certificates, username and password. Organization identifier (OI) is very important for working of STA module. STA module can communicate with roaming WLAN, however in that case the roaming WLAN must have been pre-registered and configured with home network where the STA is located.

- STA Passive Scan: The hotspot 2.0 access point sends a Beacon frame to the STA module that comprises of network type, hotspot 2.0 indication and related network information. Upon receipt of Beacon frame, the STA module checks the hotspot 2.0 indication into it. STA module can learn about basic service set (BSS) load prior to establish a connection with the access point. If all goes right, STA module performs parsing of roaming consortium field in the Beacon frame to get details about the OI of the WLAN service provider.
- STA Active Scan: During this scan, STA module sends a Probe Request frame to the access point along with the network type information. Upon receipt of this frame, access point matches with the network type of the frame with its own network type. If network type is matched, it sends the Probe Response frame to the STA module with necessary BSS load, internet connectivity flag and other network details. After receipt of Probe Response frame at the STA module, STA module checks the hotspot indication. IF everything goes right, then STA module assumes that the access point has the hotspot 2.0 facility and other activities are performed as in active scan procedure.
- STA Gathers Roaming WLAN Information: Generic advertisement service (GAS) is a mechanism that allows a STA module to exchange request and response packets with the WLAN side. Firstly, the STA sends a GAS Initial Request to the access point along with supported authentication types, hotspot 2.0 operators and related details. Upon receipt of such packet, access point responds with GAS Initial Response packet that contains ANQP structured contents such as, roaming consortium list, domain name, venue name, venue info, operator friendly name, IP address type availability, connection capacity, network authentication type information, access network type field, internet available field, BSS load information, hotspot 2.0 indication, operating class indication, network access identifier (NAI) realm, 3GPP cellular public land mobile network (PLMN), and homogeneous extended service set (HESSID).
- STA Association with Access Point: Upon detection a target WLAN, STA module sends an Association Request to the access point with NAI realm, network type, authentication types and hotspot 2.0 indication. If all goes right, access point responds back with an Association Response frame to the STA module where advanced encryption standard (AES) aware 802.1X authentication procedure is embedded.
- STA Authentication: STA module sends an 802.1X authentication request to the access point, which then forwards it to the 802.1X authentication server (AAA) via 802.1X relay (access controller) along with NAI reports. Home authentication server (AAA) then communicates with remote AAA server for requisite authentication approval. If all goes right, remote AAA server then grants access of WLAN to the STA module.

 doi:10.20944/preprints202208.0115.v1

3.4.4 Hotspot Gateway

It is a network device responsible for providing authentication, authorization, and accounting (AAA) for a given wireless network infrastructure. Despite a possible intrusion by an eavesdropper, such a gateway can prevent malicious users from accessing a private network [95]. It helps users access the Internet instantly without requiring any changes to the configuration of the user's mobile device or its internal client-side network software. With the existing network settings, a user can easily access different Internet networks through hotspot gateways. The location of the gateway can be identified by integrating the GPS -based antenna.

3.4.5 Hotspot Security Issues

Hotspot faces several challenges which can hinder the user experience as follows.

- it doesn't solve interference problems.
- it faces an installed base hurdle because, old access pint replacement is a tedious task.
- possible eavesdropping may be induced in terms of man-in-the-middle attack.
- WLAN encryption is performed at the surface or interface level, later the message travels via the underlying network stack in unencrypted manner to the remote service provider (ISP), causing risk.
- public hotspots are prone to collect the users' metadata and related content, which requires more secure access methods such as HTTPS and SSH.
- despite of authenticating users, users may be able to peek into the network traffic by using packet sniffer mechanism.
- some business vendors provide download option for Wi-Fi protected access (WPA) which may cause conflict with enterprise configurations which matches with their own WLAN specifications.

4. Distributed Hotspot Network Architecture

It is a network device responsible for providing authentication, authorization, and accounting (AAA) for a given wireless network infrastructure. Despite the possible intrusion of an eavesdropper, such a gateway can prevent malicious users from accessing a private network [95]. It helps users access the Internet instantly without requiring any changes to the configuration of the user's mobile device or its internal client-side network software. With the existing network settings, a user can easily access different Internet networks through hotspot gateways. The location of the gateway can be identified by integrating the GPS -based antenna.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 August 2022 doi:10.20944/preprints202208.0115.v1

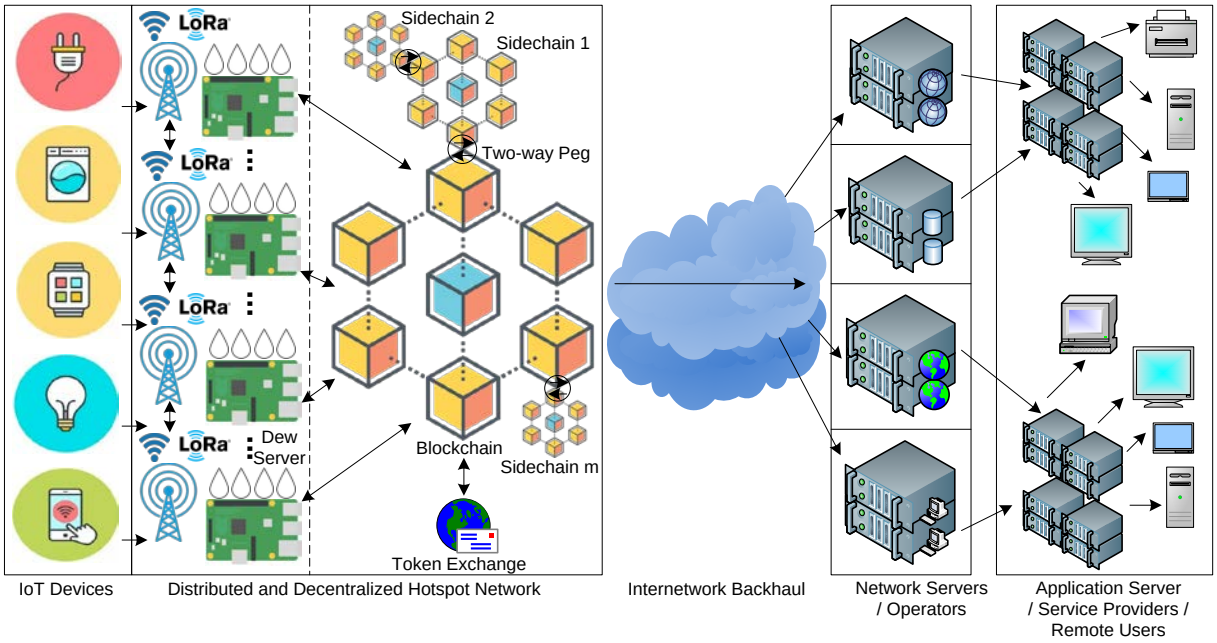

Figure 1. IoT-aware dew computing enabled blockchain assisted distributed hotspot network architecture.

4.1. IoT Device Layer

This layer includes various IoT devices from smart home, smart health, smart transportation, smart agriculture, and smart industry. All types of IoT devices along with sensors can participate in this layer. Standard 8-bit, 16-bit and 32-bit microcontrollers and microprocessor-based IoT hardware pools can be used in this layer. The main role of this layer is to transmit data packets through intermediate layers to remote application servers/service providers/users. For example, a farmer is a remote end user who can visualize, monitor or analyze the status of his farm through this architecture. He can place many devices equipped with IoT sensors at different locations on his farmland. These IoT devices are equipped with Wi-Fi and/or LoraWAN, depending on the data transmission capacities required (see above). However, it must be assumed that such IoT devices should be placed near a hotspot so that sensor data can be easily transmitted. The farmer can set up his own dew-server-centric hotspots (Wi-Fi or LoraWAN) or rent the hotspot services of others who have already set up their hotspots in the geographical coverage area of the farmer's IoT devices. In this way, the farmer's IoT devices can communicate with the remote application layer by either using the hotspot services of their own hotspots or renting the network access services of other hotspots that have been systematically placed in nearby coverage areas of such IoT devices.

4.2. Distributed and Decentralized Hotspot Network Layer

This layer is the most important layer of this architecture. The idea behind this layer is related to the commonly known People Powered Network (PPN), which is similar to what the Helium Society has developed. The goal of this layer is to enable secure IoT data transmission over the distributed hotspot network access mechanism [96-97]. The term "people" is used here because the hotspots can be used by any person who wants to provide IoT data transmissions in their hotspot coverage area. Typically, the range of IEEE 802.11n (2.4 GHz) Wi-Fi is about 50 meters. However, some long-range Wi-Fi devices are becoming available that can operate on higher GHz bands (3.6/4.9/5/5.9/60 GHz) and multiple channels. For example, Wi-Fi 6 (IEEE 802.11ax) has 600-9608 Mbps and longer

 doi:10.20944/preprints202208.0115.v1

range. LoraWAN can also be used as an alternative to Wi-Fi when data transmission over very long distances at minimum data rates is required. LoraWAN is a software communication protocol and architecture based on the Lora-based Chirp Spread Spectrum (CSS) modulation scheme. Its range can be easily extended to 10-15 km, which is far more than Wi-Fi with a data capacity of 0.3-50 kbps per channel. LoraWAN has an additional advantage over cellular or other LPWAN techniques: it offers AES protection as end-to-end encrypted messaging with lower power consumption and thus better battery life. LoraWAN operates in a bandwidth of 415/868/915 MHz in a license-free spectrum.

4.2.1. Hotspot Gateway

We can use Wi-Fi or LoraWAN as a promising hotspot provider technology because they have their own advantages over other cellular and LPWAN alternatives. All hotspots equipped with Wi-Fi or LoraWAN can be configured as gateways for IoT device data. Standard off-the-shelf hardware platforms such as Raspberry Pi 4 or higher, Bea-glebone black or higher, ASUS Tinker board, Libra Computer board AML-S905X- CC, Odroid N2+, UDOO Blot v3 and other related boards can be used as hotspot gateways. Such gateways must be equipped with a high gain Wi-Fi or LoraWAN antenna. Anyone can use such hotspot gateways to provide IoT devices in the vicinity with the network.

4.2.2. 802.1X Authentication

Authentication is a very important part in this architecture. IEEE 802.11u aware IEEE 802.1X authentication can be useful in the underlying scenario. IEEE 802.11u can support network discovery and selection by using GAS, ANQP and quality of service (QoS) map distribution facilities. Upon a client-side X.509 certification, EAP-TLS can be used to allow such clients to get securely connected with server side (AAA server). On other hand, IEEE 802.1X authentication needs to components, supplicant (STA - a IoT device), authenticator (acts as bridge between the supplicant and access point), and authentication server (AAA server) which is a trusted server. Authenticator informs the authenticator about the possibility that the supplicant is allowed to connect the network. Such AAA server can run protocols like EAP or remote authentication dial-in user service (RADIUS) in their local machines. Sometimes, it can be integrated with the authenticator device itself. The whole process of authentication involves four procedures, such as, (i) initialization: at this stage supplicant is allowed for 801.1X traffic and other data such as internet protocol and allied TCP,UDP services are dropped, (ii) initiation: in this stage the authentication process begins where authenticator transmits EAP-Request Identity frame to the local network segment at 01:80:C2:00:00:03 address, upon receipt of such frame, supplicant responds with EAP-Response frame to the authenticator with its own user identity; the authenticator then transmits this frame in form of RADIUS Access Request packet to the AAA server, (iii) EAP negotiation: in this phase, AAA servers sends a RADIUS Access Challenge packet to the authenticator with embedded EAP method, the same is forwarded to the supplicant by the authenticator; then the supplicant can start with the mentioned EAP method or can respond with non-acknowledgement frame to the authenticator, and (iv) authentication: this is the final phase where both AAA server and supplicant agree on a given EAP method wherein EAP Request and EAP Response packets are transmitted between supplicant and AAA server via authenticator, this process goes until the AAA server responds EAP-Success message inside the RADIUS Access - Accept packet to the supplicant, otherwise a RADIUS Access-Reject message is sent to the supplicant, finally upon successful authentication, the supplicant sets the post to an authorized state and normal data traffic is allowed, upon logoff by the supplicant, the authenticator sets the post to an unauthorized state.

4.2.3. Dew Server Computation

 doi:10.20944/preprints202208.0115.v1

Dew servers can be used to host such hotspot gateways. We can use hotspot gateway and dew server separately to achieve higher effectiveness and better user experience. We can also integrate both into a single system where both activities can be performed simultaneously. The main goal of using dew server is to leverage the dew computing paradigm in the periphery of the distributed hotspot network. Another idea behind the use of dew computing-enabled servers is to provide better performance capabilities in a way that is independent of Internet network services (cloud), so that the hotspot can operate seamlessly in a scenario with limited Internet access. For example, hotspots can enable nearby IoT devices to share sensor data with remote applications. Dew servers can also help IoT devices transmit sensor data in rental mode. In lease mode, a Dew server that is overloaded or performing other work can allocate its nearby hotspots to act as a gateway for said IoT device. In this way, an IoT device gains better access. If a dew hotspot is unable to serve the purpose of its nearby IoT device, it can forward coverage to the nearest dew hotspot system, which will handle message delivery for the IoT device. Another important aspect of using dew computing in this layer is the security of IoT-based messages. Such secure transmission can be ensured by incorporating a peer-to-peer (P2P) network technology, i.e., blockchain.4.2.4. Dew Server as Hotspots.

Ordinary hotspot gateways can function in two ways: (i) as a lightweight hotspot miner and (ii) as a data-only hotspot. It may not be advisable to configure an ordinary hotspot gateway as a full-fledged hotspot miner due to the following problem. It is well known that as a blockchain grows since its inception, full nodes experience a huge burden of processing and storing distributed ledgers on the local machine. Gradually, such Full Nodes tend to be out of sync with the main Blockchain. Due to the very high computational requirements, one can think about using moderately resilient miner nodes in the presented architecture. Instead of using ordinary hotspot gateways as full miners, we can consider them as lightweight hotspot miners or data-only hotspots. It is possible to turn a hotspot device into a lightweight miner along with a hotspot provisioning tool, or configure it as a data-only hotspot (without mining functionality). In our architecture, each person can deploy their Dew server to act as either a lightweight hotspot miner or a data-only hotspot broker. Dew servers can solve the synchronization problem that usually occurs with full miners. Thus, a dew server can solve this problem and opens a new way to mitigate the synchronization problems normally encountered with traditional network computers.

4.2.5. Types of Hotspots

Based on earlier discussion, we can state that the dew servers can act as (i) full hotspot miner, (ii) light-weight hotspot miner, and (iii) data-only hotspots. Anyone can deploy the dew servers to act as one of three hotspots in the aforementioned architecture. In doing so, the range of hotspot network coverage can be expanded to several hundreds of miles which can transmit an IoT data in a fraction of cost and energy with respect to standard cellular networks. All types of miners should follow same software and packet format so that homogeneity is perceived [98][99]. Besides acting as hotspot facilitator, dew severs can act as miners too. Such miners can also earn a given cryptocurrency (standard e.g., bitcoin, Ethereum, tether, USD, XRP, terra, Binance etc., or indigenously (newly) developed) from the network. We discuss the three types of hotspots.

- Full Hotspot: Dew servers which can be configured as full hotspots can be eligible to perform coverage facility to the IoT devices in their vicinity and also participate in all types of potential crypto-reward scenarios inside the network. The Proof-of-Coverage (PoC) can be seen as a dominant algorithm in such aspect. However, it should be maintained that such full hotspots should have prior approval from the underlying network authority with high-standard and failure-

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 August 2022 doi:10.20944/preprints202208.0115.v1

proof subjunctives. We apprehend that higher specification de servers with complex processor design and memory capacity are mandatory for such type of hotspots.

- Light-Weight Hotspot: Such hotspots can be configured to replace full hotspots when there is moderate load and moderate computations are needed seamlessly. Dew servers have great potential to get converted into light-weight hotspots. It can perform regular hotspot coverage and perform header-wise synchronize with the associated blockchain. In the context when overloading is perceived on light-weight hotspots, it can move-off some consensus work to the full hotspots which is then expected to act as the validator of the light-weight hotspot. Use of light-weight hotspots can simplify the network structure and enables the network ecosystem to grow rapidly.
- Data-Only Hotspot: This type of hotspots can only perform network data transfer. Transfer of data related crypto-award may be earned by such hotspots. We don't expect that data-only hotspot shall participate PoC aware reward. Thus, a permissionless approach may be incorporated in the blockchain. They start earning crypto-token as and when they are allowed to add blocks to the blockchain.

4.2.6. Proof of Coverage

The PoC is used to verify that hotspots are actually in the locations they claim to be [100]. The PoC aims to verify that hotspots are in their original locations and perform IoT device-related wireless network coverage from their specified locations. Any network that can be created using our architecture should be a physical wireless network. The success of such a physical wireless network depends on the reliability and availability of network coverage for the IoT devices in the environment. The PoC algorithm uses the key properties of some radio frequencies (RF) as evidence that the hotspots are operating as smoothly as they claim. The properties of the radio frequencies are as follows:

- Theadio frequency has a limited range for propagation.
- The radio frequency signal received at a terminal can be used to measure signal strength by applying the proportional squared distance law.
- Radio frequencies have a minimum latency because they propagate at the speed of light.

The associated blockchain periodically polls all connected hotspots using the PoC algorithm to verify that they provide stable and reliable coverage for IoT devices. In this way, the PoC confirms that the hotspots are constantly transmitting IoT data and storing it as blocks in the blockchain. Such a policy can be seen as proof that the hotspots are working while their coverage is being used for IoT devices.

The PoC essentially poses a challenge to all hotspots as a discrete unit of work of the algorithm. Several million such challenges can be issued to the hotspots and processed simultaneously by the associated blockchain [100]. With each new challenge, the PoC confirms that the hotspot network is functioning as desired. The main goal of the PoC is to minimize the PoC interval to a certain limit - α-blocks or less. At any point in time, a hotspot has one of the following three main roles:

- Interrogator: usually, such nodes are full hotspot nodes or other designated validators that create the PoC challenge and issue it to the condemned node. It challenges the PoC for a convicted target node.
- Convicted: it is a hotspot node that is the target of the PoC challenge and is expected to transmit the challenge packets so that nearby hotspots can observe its activity.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 August 2022 doi:10.20944/preprints202208.0115.v1

- Witness: such hotspots are located in the immediate (geographic) vicinity of the convicted node and also report to the querying system the status of the challenge packets sent by the convicted node (High Performance Remote Procedure Call - gRPC). Such a witness is directly connected to all lightweight hotspot nodes. Such lightweight nodes that are PoC challenge witnesses can use validators to which they are connected so that the entire query validator search process can be managed using the hash of the PoC packet. This routing information is later used by the lightweight hotspot to deliver the witness report directly to the query sender. Once the query sender receives both convicted receipts and witness reports after a certain time, it transmits them to the blockchain and the PoC challenge is complete.

4.2.7. PoC Challenge Creation and Target Selection

Ordinarily, full hotspots or validators can construct a challenge for every block of the blockchain. However, increasing such challenge request per block can be disastrous in terms of computation load. Thus, a variable - β can be used to control PoC challenge rate so that the number of PoC challenge per block can be controlled. Increasing β can significantly increase the PoC challenges in each block.

Firstly, a full hotspot or validator generates short-term key pair - *(p,q)* and a hash - *hash(publickey)*. Secondly, *(p,q)* and *hash(publickey)* are included into validator *txns*. Next, the *privatekey* is stored to *local_state(validator)*. Later, while absorbing the *txn*s, if proposed keys don't match to a consensus group member (CGM), such proposed keys are added to local cache - *lcache*. Later, each member of CGM selects a number of keys – $k \in$ *lcache* so that target β can be obtained. If minimum *2k+1* number of nodes participate in a block, then β can be obtained by following $\frac{\beta}{2(N-1)/3}$ by each of the validators in the group. The value of β may be fixed so that unnecessary change of α periodically for reducing network load. If more than 2*k+1* number of nodes participate, then public keys hashes are truncated so that block metadata can be formed. A number of selected keys are removed from *lcache*, thus resulting into the adjustment and governance by the validators to serve the capacity of the network.

Once, a block is successfully handled, every validator inspects the *publickey* in the given block and finds whether it matches with them. If match happens, a new PoC is generated for each of such matching. Later, the *hash(publickey)* is used with the *hash(block)* to generate an entropy – *e* for the perspective PoC challenge in *H3* region. Such entropy – *e* which is generated from a combination of *hash(publickey)* and *hash(block)* is used to identify the target node in the *H3* region for generating PoC challenge. All the region, PoC challenge and target are locally persistent with each challenger validator.

4.2.8. Crypto-Mining and Rewards

Dew servers acting as hotspot miners can earn crypto tokens as rewards for their reliable network coverage service for IoT devices. Such crypto tokens can have any standard form or be developed in-house. The block time can be - μ seconds and the target epoch size - b blocks. Usually, an epoch consists of all blocks processed by the current CG since the end of the last epoch. Let us assume that the blockchain is designed to mint - c crypto tokens per month. Then the following formula can be used to analyse the number of epochs per month - l and crypto-tokens per epoch - m:

l = (43200 minute per month)/((μ*b)/60 per epoch)

m = (c crypto-token per month)/(*l* epochs per month)

 doi:10.20944/preprints202208.0115.v1

The crypto token per epoch - m can be shared between the PoC interrogator, PoC convicted, and witness nodes in a standardized manner. The reward can also be split between the CG and the network (data-only hotspot) rewards associated with data transmission. Hotspot owners can use multiple crypto wallets to receive or issue crypto tokens. Such wallets may be equipped with the following features: Account balance verification, network identity verification, reconciliation, address book support, and support for payments to multiple accounts/recipients.

4.2.7. Network Consensus Protocol Goals

The network consensus protocol can be designed around the following key properties: (i) permission-free: Any hotspot that operates reliably can participate in the network architecture, (ii) constraints can be imposed so that there is no additional benefit to complex hardware equipment in the hotspot, (iii) the protocol is Byzantine fault-tolerant, (iv) the consensus system should be based on useful, reliable, and reusable actions, (v) the transaction confirmation rate should be imposed, and (vi) the hotspots should behave in a censorship-independent manner (they should not select or deselect any IoT device). In addition, the formation of sidechains can be allowed for conducting micropayments, research and development, and publishing betas. A sidechain is a blockchain that is connected to a parent blockchain via a two-way connection. Such sidechains have their own consensus protocols so that privacy and security can be improved. In this way, trust in the main blockchain is minimized. The two-way connection facilitates the transfer of digital assets between blockchains. In addition, such blockchains can enable the exchange of crypto tokens.4.3. Internetwork Backhaul

Internetworking for incoming messages from IoT devices via various hotspots and blockchain are transmitted to target application server / remote users. This internetwork backhaul can be optional, if the LoraWAN aware design is considered where LoraWAN-based platforms can act as the message delivery supported. For example, Helium channels can be deployed to serve the backhaul connectivity to remote network servers/operators. Standard the things network (TTN) is also capable to perform similar tasks. Otherwise, regular cellular-based internetwork backhaul may be considered.

4.4. Network Servers/Operators

Network servers/operators are the entities, the standard ISPs, that can be used in this architecture as domain name servers or path forwarders. Such providers enable wireless bearer services, especially cellular services for the end applications or users. To accomplish this task, the operators perform radio frequency allocation, end-user support, network process maintenance, and network equipment provisioning. These operators are also able to generate revenue and charge end-applications or customers according to their agreement or network usage policy. In addition, mobile virtual network operators (MVNOs) can be used as leased network service providers under the major network operators.

4.5. Application Servers/ Service Providers/Remote Users

Application servers host applications and/or software to provide business applications to their subscribers or end users. Such servers may use the server framework service model through an application programming interface (API) to accomplish the desired task. In general, application servers are built to be fail-safe and can perform load balancing. Mobile

 doi:10.20944/preprints202208.0115.v1

application servers (MAS) can also be used to augment business logic with representative state transfer (REST) so that bandwidth can be minimized. In addition, MAS can provide authentication services, offline support, security, and data orchestration. Service-oriented architecture (SOA)-oriented infrastructures are capable of connecting to dependent end users, but limited resources and broken connections can cause problems.

5. Discussion

Our architecture is inspired by the design of the Helium integration network, where IoT devices can transmit sensor data to remote application servers or users. We modified the design of the architecture in a multi-layered manner to achieve more control over the network. Our architecture represents a true hotspot coverage network in which many hotspots can be placed within the coverage area of each hotspot. In this way, IoT devices can transmit messages on a hop-by-hop basis. We use the dew computing paradigm to minimize Internet dependency and improve accessibility for end devices. The hotspots can be integrated with dew servers to enhance the ability to act as one of three types of hotspots, such as (i) full-fledged hotspot miner, (ii) lightweight hotspot miner, and (iii) data-only hotspot. A dew-enabled hotspot can earn crypto tokens based on its specified activities.

The implicit architecture enables a new type of incentive for hotspot owners to set up hotspots according to their needs. Dew Computing leverages the synchronization aspect, which does not require a direct Internet connection. Dew Computing hotspots can communicate with each other to create a distributed ad hoc network that operates independently of the Internet. This provides high reliability and availability for IoT devices that want to transmit sensor data to remote locations. IoT devices do not need to be directly connected to the Internet, which can dramatically reduce costs and traffic on the cellular network. Our architecture provides two types of hotspot technologies (i) Wi-Fi and (ii) LoraWAN. Wi-Fi enabled tau-based hotspot miners can be used when high data speed is required and there is an Internet connection between the hotspot network layer and the remote network service providers or end users. LoraWAN can be used when a low data rate is required and there may not be an Internet connection. The Thing network can be added as an exchange. Various APIs can be integrated into the LoraWAN-enabled network platforms to forward the IoT sensor data to the remote network servers and application processes.

Key Challenges:

- The architecture is a conceptual model thus it needs to be implemented. Implementation of this architecture shall require dedicated dew servers, hotspot coverage antenna like Wi-Fi and LoraWAN. Selection of Wi-Fi module could be judiciously done so that long range coverage can be facilitated with higher bandwidth. However, such antenna should consume low power for providing better sustainability. LoraWAN could be a great choice in this regard, however the cost of antenna module could be high for very long-range coverage.
- IoT devices should have Wi-Fi or LoraWAN connectivity to communicate to the nearby hotspots. Thus, serious consideration should be made so that cost of IoT device doesn't go beyond certain limit and battery consumption could be minimized.
- Hotspots need to be configured as miner nodes that should run on top of dew servers. Synchronization algorithms should be devised for making the internet independency more reliable.
- Several LoraWAN platforms including TTN, Helium, LORIOT, ResIOT, SenRa, ChirpStack can be considered while considering the internetwork backhaul. For Wi-Fi hotspots, standard cellular backhaul may be used.

- The type of blockchain should be devised. A hybrid approach can be beneficial in this aspect. An owner of hotspot miner device can place it in his locality to act as one of three types of hotspots namely full, light-weight, or data-only. Design specifications of each type of hotspot is different as their task is different. Complex, moderate and simple hotspot hardware designs should be selected prior deploying them in the real field of application.
- Concise decision should be made about the use of PoC challenging aspect in this architecture. The PoC challenge rate, epoch size and block time are important parameter that must be resolved a-priori.
- One should consider the wallet type while aiming to connect his hotspot miner node with this network architecture.
- Network consensus algorithm can be revisited to improve the reliability of the hotspot network. Target crypto-token production per unit of time (month, quarter, half yearly, yearly) need to be accorded.
- It is important to select a crypto-currency which is will be used in this architecture for rewarding the hotspot owners. It can be selected from existing standard crypto-currencies or can be devised indigenously for a specific hotspot distributed network architecture.
- The structure of block should be designed optimally. Number of transactions per block should be decided before using blocks in reality. Decision should be taken for fixing transaction fees. Oracles should be highly decided for specifying data credit conversion rate. Price of selected crypto-oracles must be aligned with other blockchain networks.
- Interoperability issues should be tackled so that this architecture can talk with other blockchains.
- Trustless packet purchasing features should be formulated in order to allow higher coverage for the hotspot network. State channels and organizationally unique identifier (OUI) should be implemented with proper care.
- Reward scaling approach must be put in place for each epoch. In this aspect, it becomes important to specify who gets what i.e., a hotspot shall earn how much reward.
- Selection of higher-grade Byzantine fault tolerant protocol becomes inevitable when blockchain is used. An asynchronous atomic broadcast protocol can be used with a consensus group which has known nodes. Threshold encryption technique may be deployed to improve the async behavior.
- Procedure should be designed to elect consensus group. It can be done epoch wise or time duration manner. Number of members of each consensus group should be judiciously decided.
- Overall governance of the hotspot network must be catered with regular voting and community meant guidelines.

Future Scope:

The architecture has the potential to enable a new type of hotspot network deployment in the future. Ordinary mobile and physical network objects should be included in the current hotspot network structure. The security features of hotspots should be considered. The architecture is expected to provide a large area as distributed coverage for the hotspots. Therefore, it is required that all hotspots follow similar rules and software updates. Edge computing devices need to be evaluated for their suitability as an alternative hotspot machine. Third-party cloud service providers can be considered to add value to this architecture.

 doi:10.20944/preprints202208.0115.v1

6. Conclusion

We discuss the possibility of deploying a novel distributed architecture that provides secure hotspot coverage for IoT devices over long distances. The distributed architecture can open a new business model where the benefits of Wi-Fi and LoraWAN technologies can be leveraged to provide a financial advantage to hotspot owners who wish to lease their hotspots for inclusion in the network. We encourage academics, researchers, and companies to develop new ideas and practical use cases based on the proposed architecture.

Author Contributions: P.P.Ray wrote the paper, designed the architecture, described the notions of the architecture, pointed out key challenges and future way outs. K. Skala helped with concept and mentoring, screening and language improvement the paper.

References

1. Ogonji, M.M., Okeyo, G. and Wafula, J.M., 2020. A survey on privacy and security of Internet of Things. Computer Science Review, 38, p.100312.Ogonji, M.M., Okeyo, G. and Wafula, J.M., 2020. A survey on privacy and security of Internet of Things. Computer Science Review, 38, p.100312.
2. Lombardi, M., Pascale, F. and Santaniello, D., 2021. Internet of things: A general overview between architectures, protocols and applications. Information, 12(2), p.87.
3. Raj, M., Gupta, S., Chamola, V., Elhence, A., Garg, T., Atiquzzaman, M. and Niyato, D., 2021. A survey on the role of Internet of Things for adopting and promoting Agriculture 4.0. Journal of Network and Computer Applications, 187, p.103107.
4. Lee, E., Seo, Y.D., Oh, S.R. and Kim, Y.G., 2021. A Survey on Standards for Interoperability and Security in the Internet of Things. IEEE Communications Surveys & Tutorials, 23(2), pp.1020-1047.
5. Ratta, P., Kaur, A., Sharma, S., Shabaz, M. and Dhiman, G., 2021. Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives. Journal of Food Quality, 2021.
6. Ogonji, M.M., Okeyo, G. and Wafula, J.M., 2020. A survey on privacy and security of Internet of Things. Computer Science Review, 38, p.100312.
7. Misra, N.N., Dixit, Y., Al-Mallahi, A., Bhullar, M.S., Upadhyay, R. and Martynenko, A., 2020. IoT, big data and artificial intelligence in agriculture and food industry. IEEE Internet of Things Journal.
8. Laghari, A.A., Wu, K., Laghari, R.A., Ali, M. and Khan, A.A., 2021. A review and state of art of Internet of Things (IoT). Archives of Computational Methods in Engineering, pp.1-19.
9. Sobin, C.C., 2020. A survey on architecture, protocols and challenges in IoT. Wireless Personal Communications, 112(3), pp.1383-1429.
10. Hossein Motlagh, N., Mohammadrezaei, M., Hunt, J. and Zakeri, B., 2020. Internet of Things (IoT) and the energy sector. Energies, 13(2), p.494.
11. Khalaf, O.I., Romero, C.A.T., Hassan, S. and Iqbal, M.T., 2022. Mitigating hotspot issues in heterogeneous wireless sensor networks. Journal of Sensors, 2022.
12. Dolan, E. and Widayanti, R., 2022. Implementation Of Authentication Systems On Hotspot Network Users To Improve Computer Network Security. International Journal of Cyber and IT Service Management, 2(1), pp.88-94.
13. Jiang, Y., Yang, F., Yu, B., Zhou, D. and Zeng, X., 2020. Efficient layout hotspot detection via binarized residual neural network ensemble. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 40(7), pp.1476-1488.
14. Swedha, S. and Gopi, E.S., 2021. LSTM network for hotspot prediction in traffic density of cellular network. In Machine Learning, Deep Learning and Computational Intelligence for Wireless Communication (pp. 35-47). Springer, Singapore.
15. Gushev, M., 2020. Dew computing architecture for cyber-physical systems and IoT. Internet of things, 11, p.100186.
16. Singh, P., Kaur, A., Aujla, G.S., Batth, R.S. and Kanhere, S., 2020. Daas: Dew computing as a service for intelligent intrusion detection in edge-of-things ecosystem. IEEE Internet of Things Journal, 8(16), pp.12569-12577.
17. Hirsch, M., Mateos, C., Zunino, A., Majchrzak, T.A., Grønli, T.M. and Kaindl, H., 2021. A task execution scheme for dew computing with state-of-the-art smartphones. Electronics, 10(16), p.2006.
18. Ahammad, I., Khan, A.R. and Salehin, Z.U., 2021. A Review on Cloud, Fog, Roof, and Dew Computing: IoT Perspective. International Journal of Cloud Applications and Computing (IJCAC), 11(4), pp.14-41.
19. Wang, Y., 2020. A blockchain system with lightweight full node based on dew computing. Internet of Things, 11, p.100184.
20. Manocha, A., Bhatia, M. and Kumar, G., 2021. Dew computing-inspired health-meteorological factor analysis for early prediction of bronchial asthma. Journal of Network and Computer Applications, 179, p.102995.
21. Hirsch, M., Mateos, C., Rodriguez, J.M. and Zunino, A., 2020. DewSim: A trace-driven toolkit for simulating mobile device clusters in Dew computing environments. Software: Practice and Experience, 50(5), pp.688-718.

22. Moussa, M.M. and Alazzawi, L., 2020, November. Cyber attacks detection based on deep learning for cloud-dew computing in automotive iot applications. In 2020 IEEE International Conference on Smart Cloud (SmartCloud) (pp. 55-61). IEEE.
23. Draz, U., Ali, T., Yasin, S., Waqas, U. and Rafiq, U., 2019, February. EADSA: Energy-aware distributed sink algorithm for hotspot problem in wireless sensor and actor networks. In 2019 international conference on engineering and emerging technologies (ICEET) (pp. 1-6). IEEE.
24. Ye, A., Li, Q., Zhang, Q. and Cheng, B., 2020. Detection of spoofing attacks in WLAN-based positioning systems using WiFi hotspot tags. IEEE Access, 8, pp.39768-39780.
25. Wang, X., Lin, F. and Wu, Y., 2019, January. A novel positioning system of potential WiFi hotspots for software defined WiFi network planning. In 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-6). IEEE.
26. Noura, H., Hatoum, T., Salman, O., Yaacoub, J.P. and Chehab, A., 2020. LoRaWAN security survey: Issues, threats and possible mitigation techniques. Internet of Things, 12, p.100303.
27. Jouhari, M., Amhoud, E.M., Saeed, N. and Alouini, M.S., 2022. A Survey on Scalable LoRaWAN for Massive IoT: Recent Advances, Potentials, and Challenges. arXiv preprint arXiv:2202.11082.
28. Zhou, Q., Huang, H., Zheng, Z. and Bian, J., 2020. Solutions to scalability of blockchain: A survey. Ieee Access, 8, pp.16440-16455.
29. Syed, T.A., Alzahrani, A., Jan, S., Siddiqui, M.S., Nadeem, A. and Alghamdi, T., 2019. A comparative analysis of blockchain architecture and its applications: Problems and recommendations. IEEE access, 7, pp.176838-176869.
30. Zheng, W., Zheng, Z., Chen, X., Dai, K., Li, P. and Chen, R., 2019. NutBaaS: a blockchain-as-a-service platform. Ieee Access, 7, pp.134422-134433.
31. Wang, Q., Zhu, X., Ni, Y., Gu, L. and Zhu, H., 2020. Blockchain for the IoT and industrial IoT: A review. Internet of Things, 10, p.100081.
32. Singh, S., Hosen, A.S. and Yoon, B., 2021. Blockchain security attacks, challenges, and solutions for the future distributed iot network. IEEE Access, 9, pp.13938-13959.
33. Zha, D.S., Feng, T.T., Gong, X.L. and Liu, S.Y., 2022. When energy meets blockchain: A systematic exposition of policies, research hotspots, applications, and prospects. International Journal of Energy Research, 46(3), pp.2330-2360.
34. Zhao, X., Lei, Z., Zhang, G., Zhang, Y. and Xing, C., 2020, September. Blockchain and distributed system. In International Conference on Web Information Systems and Applications (pp. 629-641). Springer, Cham.
35. Messié, V., Fromentoux, G., Labidurie, N., Radier, B., Vaton, S. and Amigo, I., 2022. BALAdIN: truthfulness in collaborative access networks with distributed ledgers. Annals of Telecommunications, 77(1), pp.47-59.
36. Lopez, D., Yazdizadeh, A., Farooq, B. and Patterson, Z., 2019, July. Distributed Privacy-Aware Choice Modelling using Federated Learning over Blockchain. In International Choice Modelling Conference 2019.
37. Janiesch, C., Fischer, M., Imgrund, F., Hofmann, A. and Winkelmann, A., An Architecture Using Payment Channel Networks for Blockchain-based Wi-Fi Sharing: An Architecture for Blockchain-based Wi-Fi Sharing. ACM Transactions on Management Information Systems.
38. Yang, Y., Liu, Z., Liu, Z., Chan, K.Y. and Guan, X., 2022. Joint Optimization of Edge Computing Resource Pricing and Wireless Caching for Blockchain-Driven Networks. IEEE Transactions on Vehicular Technology, 71(6), pp.6661-6670.
39. Zhao, Z., Guo, J., Luo, X., Xue, J., Lai, C.S., Xu, Z. and Lai, L.L., 2020. Energy transaction for multi-microgrids and internal microgrid based on blockchain. IEEE Access, 8, pp.144362-144372.
40. Kim, S.K.S., 2019. Apply Blockchain to Overcome Wi-Fi Vulnerabilities. Journal of Multimedia Information System, 6(3), pp.139-146.
41. Ivanov, N., Lou, J. and Yan, Q., 2020, October. Smart wifi: Universal and secure smart contract-enabled wifi hotspot. In International Conference on Security and Privacy in Communication Systems (pp. 425-445). Springer, Cham.
42. Pustišek, M., Dolenc, D. and Kos, A., 2019. LDAF: Low-bandwidth distributed applications framework in a use case of blockchain-enabled IoT devices. Sensors, 19(10), p.2337.
43. Ma, S., Li, H., Yang, W., Li, J., Nepal, S. and Bertino, E., 2020, December. Certified Copy? Understanding Security Risks of Wi-Fi Hotspot based Android Data Clone Services. In Annual Computer Security Applications Conference (pp. 320-331).
44. Casado-Vara, R., Novais, P., Gil, A.B., Prieto, J. and Corchado, J.M., 2019. Distributed continuous-time fault estimation control for multiple devices in IoT networks. IEEE Access, 7, pp.11972-11984.
45. Babun, L., Denney, K., Celik, Z.B., McDaniel, P. and Uluagac, A.S., 2021. A survey on IoT platforms: Communication, security, and privacy perspectives. Computer Networks, 192, p.108040.
46. Boursianis, A.D., Papadopoulou, M.S., Diamantoulakis, P., Liopa-Tsakalidi, A., Barouchas, P., Salahas, G., Karagiannidis, G., Wan, S. and Goudos, S.K., 2022. Internet of things (IoT) and agricultural unmanned aerial vehicles (UAVs) in smart farming: A comprehensive review. Internet of Things, 18, p.100187.
47. Lounis, K. and Zulkernine, M., 2020. Attacks and defenses in short-range wireless technologies for IoT. IEEE Access, 8, pp.88892-88932.
48. Wang, Q., Zhu, X., Ni, Y., Gu, L. and Zhu, H., 2020. Blockchain for the IoT and industrial IoT: A review. Internet of Things, 10, p.100081.
49. Alshehri, F. and Muhammad, G., 2020. A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare. IEEE Access, 9, pp.3660-3678.

50. Husnoo, M.A., Anwar, A., Chakrabortty, R.K., Doss, R. and Ryan, M.J., 2021. Differential privacy for IoT-enabled critical infrastructure: A comprehensive survey. IEEE Access.
51. Mohanta, B.K., Jena, D., Satapathy, U. and Patnaik, S., 2020. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 11, p.100227.
52. Nižetić, S., Šolić, P., González-de, D.L.D.I. and Patrono, L., 2020. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. Journal of Cleaner Production, 274, p.122877.
53. Chettri, L. and Bera, R., 2019. A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. IEEE Internet of Things Journal, 7(1), pp.16-32.
54. Hassan, W.H., 2019. Current research on Internet of Things (IoT) security: A survey. Computer networks, 148, pp.283-294.
55. Wu, M., Wang, K., Cai, X., Guo, S., Guo, M. and Rong, C., 2019. A comprehensive survey of blockchain: From theory to IoT applications and beyond. IEEE Internet of Things Journal, 6(5), pp.8114-8154.
56. Pavithran, D., Shaalan, K., Al-Karaki, J.N. and Gawanmeh, A., 2020. Towards building a blockchain framework for IoT. Cluster Computing, 23(3), pp.2089-2103.
57. Gill, S.S., Tuli, S., Xu, M., Singh, I., Singh, K.V., Lindsay, D., Tuli, S., Smirnova, D., Singh, M., Jain, U. and Pervaiz, H., 2019. Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. Internet of Things, 8, p.100118..
58. Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R.C., Michelin, R.A., Zorzo, A.F. and Kanhere, S.S., 2020. Blockchain technologies for iot. In Advanced applications of blockchain technology (pp. 55-89). Springer, Singapore.
59. Shahbazi, Z. and Byun, Y.C., 2021. Integration of Blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing. Sensors, 21(4), p.1467.
60. Rane, S.B. and Thakker, S.V., 2020. Green procurement process model based on blockchain–IoT integrated architecture for a sustainable business. Management of Environmental Quality: An International Journal.
61. Si, H., Sun, C., Li, Y., Qiao, H. and Shi, L., 2019. IoT information sharing security mechanism based on blockchain technology. Future Generation Computer Systems, 101, pp.1028-1040.
62. Tseng, L., Yao, X., Otoum, S., Aloqaily, M. and Jararweh, Y., 2020. Blockchain-based database in an IoT environment: challenges, opportunities, and analysis. Cluster Computing, 23(3), pp.2151-2165.
63. Alladi, T., Chamola, V., Parizi, R.M. and Choo, K.K.R., 2019. Blockchain applications for industry 4.0 and industrial IoT: A review. IEEE Access, 7, pp.176935-176951.
64. Sun, S., Du, R., Chen, S. and Li, W., 2021. Blockchain-based IoT access control system: towards security, lightweight, and cross-domain. IEEE Access, 9, pp.36868-36878.
65. Sharma, P.K., Kumar, N. and Park, J.H., 2020. Blockchain technology toward green IoT: Opportunities and challenges. IEEE Network, 34(4), pp.263-269.
66. Hirsch, M., Mateos, C., Zunino, A., Majchrzak, T.A., Grønli, T.M. and Kaindl, H., 2021. A task execution scheme for dew computing with state-of-the-art smartphones. Electronics, 10(16), p.2006.
67. Ahammad, I., Khan, A.R. and Salehin, Z.U., 2021. A Review on Cloud, Fog, Roof, and Dew Computing: IoT Perspective. International Journal of Cloud Applications and Computing (IJCAC), 11(4), pp.14-41.
68. Gusev, M., 2021, July. Serverless and Deviceless Dew Computing: Founding an Infrastructureless Computing. In 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 1814-1818). IEEE.
69. Gusev, M., 2021, July. What makes Dew computing more than Edge computing for Internet of Things. In 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 1795-1800). IEEE.
70. Javadzadeh, G., Rahmani, A.M. and Kamarposhti, M.S., 2022. Mathematical model for the scheduling of real-time applications in IoT using Dew computing. The Journal of Supercomputing, 78(5), pp.7464-7488.
71. Sverko, M., Tankovic, N. and Etinger, D., 2021, July. Dew Computing in Industrial Automation: Applying Machine Learning for Process Control. In 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 1789-1794). IEEE.
72. Braeken, A., 2022. Authenticated key agreement protocols for dew-assisted IoT systems. The Journal of Supercomputing, pp.1-21.
73. Raza, H., Amjad, M. and Muneer, S., 2022. IoT Based Cyber-Physical System in Automobile Devices with Dew Computing Architecture. Journal of NCBAE, 1(1).
74. Yu, Y.C., 2021, July. A Dew Computing Architecture for Smart Parking System with Cloud Image Recognition Service. In 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 1805-1809). IEEE.
75. Gusev, M., 2022. AI cardiologist at the edge: A use case of a dew computing heart monitoring solution. In Artificial Intelligence and Machine Learning for EDGE Computing (pp. 469-477). Academic Press.
76. Rana, S., Obaidat, M.S., Mishra, D., Mishra, A. and Rao, Y.S., 2022. Efficient design of an authenticated key agreement protocol for dew-assisted IoT systems. The Journal of Supercomputing, 78(3), pp.3696-3714..
77. Medhi, K., Ahmed, N. and Hussain, M.I., 2021. Dew-based offline computing architecture for healthcare IoT. ICT Express.
78. Guberović, E., Lipić, T. and Čavrak, I., 2021, July. Dew Intelligence: Federated learning perspective. In 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 1819-1824). IEEE.

79. Aishwarya, M.R. and Mathivanan, G., 2021, December. AI Strategy for Stake Cloud Computing and Edge Computing: A State of the art survey. In 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 920-927). IEEE.
80. Aburukba, R., Al-Ali, A.R., Riaz, A.H., Al Nabulsi, A., Khan, D., Khan, S. and Amer, M., 2021. Fog Computing Approach for Shared Mobility in Smart Cities. Energies, 14(23), p.8174.
81. Escobar-Diaz, F., Buitrago, C., Quiñones, L., Grajales, F. and Mejia, T., 2021, November. Evaluation of particulate matter microsensors to build the low-cost sensors collaborative network of Bogotá. In 2021 Congreso Colombiano y Conferencia Internacional de Calidad de Aire y Salud Pública (CASAP) (pp. 1-5). IEEE.
82. Aburukba, R., Al-Ali, A.R., Riaz, A.H., Al Nabulsi, A., Khan, D., Khan, S. and Amer, M., 2021. Fog Computing Approach for Shared Mobility in Smart Cities. Energies 2021, 14, 8174.
83. Dong, W., Lv, J., Chen, G., Wang, Y., Li, H., Gao, Y. and Bharadia, D., 2022, June. TinyNet: a lightweight, modular, and unified network architecture for the internet of things. In Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services (pp. 248-260).
84. Veloso, A.F.D.S., Júnior, J.V.R., Rabelo, R.D.A.L. and Silveira, J.D.F., 2021. HyDSMaaS: A Hybrid Communication Infrastructure with LoRaWAN and LoraMesh for the Demand Side Management as a Service. Future Internet, 13(11), p.271.
85. Schütz, M., 2021, October. RF Harvesting at 2.4 GHz for Scattering between Battery-less Transponder and Mobile Telephones. In 2021 IEEE International Conference on RFID Technology and Applications (RFID-TA) (pp. 93-96). IEEE.
86. Mishra, V.K., Swami, B.D., Kanagarathinam, M.R., Thorat, P.B. and Das, D., 2019, April. NextGen-MHS: A Novel Architecture for Tethering of Aggregated Licensed and Unlicensed Spectrums. In 2019 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE.
87. Agyemang, J.O., Kponyo, J.J., Klogo, G.S. and Boateng, J.O., 2020. Lightweight rogue access point detection algorithm for WiFi-enabled Internet of Things (IoT) devices. Internet of Things, 11, p.100200.
88. Xu, W., Zhou, H., Bi, Y., Cheng, N., Shen, X., Thanayankizil, L. and Bai, F., 2018. Exploiting hotspot-2.0 for traffic offloading in mobile networks. IEEE Network, 32(5), pp.131-137.
89. Nojima, D. and Yamada, A., 2019. Technologies for Interworking Between Cellular and WLAN Systems. IEICE Communications Society GLOBAL NEWSLETTER Vol. 43, No. 2, p.3.
90. Bednarczyk, M., 2019, March. IEEE 802.11 ax: giant leap in WLAN evolution. In XII Conference on Reconnaissance and Electronic Warfare Systems (Vol. 11055, pp. 416-422). SPIE.
91. Xu, W., Zhou, H., Bi, Y., Cheng, N., Shen, X., Thanayankizil, L. and Bai, F., 2018. Exploiting hotspot-2.0 for traffic offloading in mobile networks. IEEE Network, 32(5), pp.131-137.
92. Backhaus, M., Theil, M., Rossberg, M. and Schaefer, G., 2020. Improving Network-Assisted Roaming for Controller-Less Wi-Fi. In 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications (pp. 1-7). IEEE.
93. Hidayat, T.N. and Riadi, I., 2021. Optimation wireless security IEEE 802.1 X using the extensible authentication protocol-protected extensible authentication protocol (EAP-PEAP). International Journal of Computer Applications, 174(11), pp.25-30.
94. Huawei Hotspot 2.0, https://support.huawei.com/enterprise/en/doc/EDOC1100096325/2010a98b/understanding-hotspot-20, Accessed on July 16, 2022.
95. Paolini, A., Scardaci, D., Liampotis, N., Spinoso, V., Grenier, B. and Chen, Y., 2020. Authentication, authorization, and accounting. Towards Interoperable Research Infrastructures for Environmental and Earth Sciences, pp.247-271.
96. Helium network, https://docs.helium.com/, Accessed on July 15, 2022.
97. Helium mining, https://www.okdo.com/blog/the-ultimate-guide-to-lora-helium-miners-and-crypto-mining/, Accessed on July 16, 2022.
98. Helium network design, https://create.arduino.cc/projecthub/akarsh98/what-is-helium-network-hnt-mining-hotspots-and-crypto-7a148e, Accessed on July 16, 2002.
99. Helium hotspot mining, https://create.arduino.cc/projecthub/akarsh98/tutorial-helium-light-hotspot-with-dragino-lps8-dlos8-miner-b7a39e, Accessed on July 16, 2002.
100. Proof of coverage, https://docs.helium.com/blockchain/proof-of-coverage, Accessed July 15, 2022.
101. Helium network white paper, http://whitepaper.helium.com/, Accessed July 14, 2022.