IJCSN - International Journal of Computer Science and Network, Volume 9, Issue 5, October 2020
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Integration of Fog Computing with Internet of Things (IoT): Blockchain Perspectives

[1] Srishti Garg; [2] P. K. Chaurasia

[1] Department of Information Technology,
Babasaheb Bhimrao Ambedkar University, Lucknow

[2] Department of Computer Science & Information Technology
Mahatma Gandhi Central University, Motihari, Bihar, (India)

Abstract - The predominantly global stationing and utilization of technologically advanced and interactive electronic devices such as the tablets, phablets, smart phones, refrigerators, sensors, speakers, etc. These are mainly interrelated channelization of various applications for the Internet of Things (IoT) devices are reckoned to outstretch a large indefinite amount, from last two decades. The biggest challenge is the management of such amounts of data, which seems to be unable to be coped up with the user of traditional IoT and cloud-based architectures. A solution to this is the decentralization of applications using a computed distributed model. The infrastructure generating big data or a fog-based architecture which extends the Cloud Computing paradigm is defined to fully support the IoT methodology. Fog computing or "Fogging" works with the aim to enhance the processing, intelligence, and accumulation of data gradually closer and streamlined to the Edge of a network. This facilitates to provide computer-related services more efficiently much closer to the inter-operated smart things that form a major part of the IoT in a distributed computed environment. The objective of this paper is to understand the topical impediments which arise in the critical infrastructure of the organization's technology systems. Further, after introduction of the infrastructure, the challenges in securing and maintaining the big data privacy and trust concerns in relation to fog-enabled IoT is presented. A blockchain-based technology is deployed to address the security related issues in IoT and fog computing. Thereafter, Blockchain is integrated with IoT applications. The work, therefore, formalizes task of securing data in the current scenario, the prevalent threats for practitioners and the recommendations for promising research investigation in the future.

Keywords - *Blockchain, Big Data, Cloud Computing, Fog Computing, Internet of Things (IoT), Security*.

1. Introduction

The physical "things" and other objects with highly intuitive proficiency, digital objects such as smart phones, automobiles and other vehicles, electronic devices which are customer- oriented, and various other gadgets similar to refrigerators, televisions, and healthcare devices are being advantaged within the limits of the Internet environment through the lens of Internet of Things (IoT) paradigm [1]. The cloud centric IoT (CIoT) applications work by extraction, accumulation and processing of the sensor data from these "things" is extracted at the public/private clouds which promotes to the rise of significant latencies [2].

The issue of latency in developing real-time IoT applications which is mainly done by utilizing proximity-based computational resources across the IoT layers such as gateways, cloudlets, and network switches/routers is addressed by the artistry of fog computing. To exploit the full potential of fog computing and similar paradigms, researchers and practitioners need to tackle several challenges and develop suitable conceptual and technological solutions for addressing the various issues. These complications might include development of scalable architectures, movement from closed systems to open systems, handling privacy and ethical issues involved in data sensing, storage, processing, designing of interaction protocols and autonomic management [3]. Thus, the foreseen current issues and in-hand challenges envision to be the prime motivation in the formulation of the paper discussing the future anticipations in context with fog computing

This paper is divided into nine sections: First section is the introduction of the fog computing, internet of things and blockchain technology, second section is, how to evolve fog computing with IoT and cloud computing, third section is defined the architecture of fog computing, fourth section fog-enabled distributed model, fifth section is the issues of fog computing, sixth section is the challenges of fog computing description, seventh section is security of blockchain, eighth section is the future research direction and final section is the conclusion of the research.

The IoT envisions a completely connected world, where things can convey estimated information and collaborate with one another. This makes conceivable an advanced digital representation of this present reality, through which many savvy applications in an assortment of businesses can be developed. In the Internet of Things (IoT) vision, regular gadgets become brilliant and self-contained. This vision is transforming into a reality because of advances in innovation, yet there are still difficulties to address, especially in the security realm e.g., information reliability. Fog Computing is a disseminated computing scenario that stretches out the Cloud computing worldview to completely uphold the Internet of Things (IoT) vision. It expects to push the intellect, process handling and storage capacity of information closer to the Edge of the webwork to give computer-related solutions all the more quickly and close to the interconnected smart things that structure part of the IoT. Considering the anticipated advancement of the IoT in the upcoming years, it is imperative to confer self-reliance in this enormous approaching data source. Blockchain has developed as a key innovation that will revolutionize how we carve up information. Satoshi Nakamoto, in 2008 [3] introduced two extremist ideas that have had an extraordinary repercussion. The first of these is Bitcoin, a virtual digital currency that keeps up its incentive without aid from any centralized power or money-related entity. Moderately, the currency is held altogether and safely by a decentralized "Peer to Peer" (P2P) web of actors that make up an auditable [3] and certifiable network. The second of the ideas, whose ubiquity has gone significantly farther than the cryptocurrency itself, is Blockchain.

Blockchain is the instrument that permits exchanges to be confirmed by an assembly of variable actors. It gives a dispersed, irretrievable, see-through, secure, and auditable testimony (ledger). The blockchain can be conferred transparently and completely, permitting admittance to all exchanges that have happened since the principal transaction of the framework can be chequeen and assembled by any entity each time. Building trust in dispersed circumstances without the requirement for professionals is a technological development that can possibly change numerous ventures, the IoT among them.

2. Fog Computing

The exchange of data in large number of physical "things", which are encapsulated with devices likewise the detectors, transducers etc. amidst each other or the Internet throughout variegated wide-ranging networks, ushers to the epoch of the "Internet of Things" (IoT) [4]. Currently, the interdependence between various smart devices, which probably smart speakers, phones, cards, home appliances like refrigerators, doorbells, traffic lights, wearable devices like smart watches and bands, vehicles like smart cars, various industrial sensors propound to give diverse and heterogeneous resources and other relevant practical applications in different dominions, encompassing various diversities of smart cities, healthcare industry administered digitally, transportation regulated intuitively and so forth and so on [4]. This metamorphic revolution aims to bring new opportunities promoting in the development of our society and improving the living standards. But with numerous devices being associated simultaneously, there is a tremendous increase in data production from diverse services and applications, which marshals to enhance an overwhelming and gigantic pressure on data banks, database operation, data inspection and perusal. Various speculations forecast; smart devices linked to the cyberspace would generate data fabricated to 507.5 ZB per year. In turn data progressed from the devices to the cloud will demand prerequisites analogous to immense amounts of transmission bandwidth, substantial storage repositories and other miscellaneous computational resources [5, 6]. However, second sights foretell is quite feasible to maintain and process 45% of produced data at the edge of the network locally or within close range of the devices. Furthermore, it is important that all the produced data should be analyzed within regulated time duration to ascertain the knowledge for fulfilling the application stipulations by locally managing the stockpiles for real-time decision. It is to be, therefore, considered that data storage and analysis which happens to be in a centralized manner is unable to furnish the requirements of data-driven requisitions and slumbered responses of resources [7]. Fog computing [8] has been initiated to empower data-driven services and latency-sensitive applications, by pushing data depositories and organizational resources to the critical edge of the network. Towards the communication networks which are more stereotypical, the progression significantly aims to emphasize in establishing the connection proficiently, network guide and other amenities linking the end devices more locally cloud [9]. Headings are to be column centered in a bold font without underline. They need be numbered. "2. Headings and Footnotes" at the top of this paragraph is a major heading.

Fog computing a term coined by Cisco in 2012 is defined to be a diversification of cloud computing that delivers multifarious utilities of computation, storage, and low latency, and high bandwidth, awareness of the location,

networking amenities which are amongst end devices and cloud servers and other local time conveniences to IoT services [9, 10].

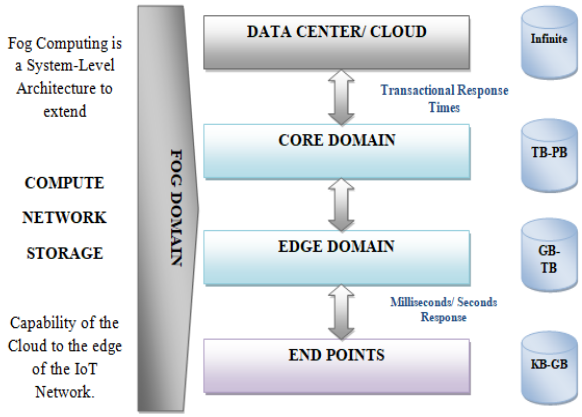

Figure 1: Fog Computing in IoT and Cloud Computing Environment

Fig.1 describes the system level architecture of fog computing. Fogs facilitate a fundamental hierarchical foundation structure, which operate by movement of data, its subsequent storage and analysis of local data being performed at fogs, and perpetual storage and more comprehensive probing occurring at the cloud. Fogging entirely complements the cloud environment. With keeping the elementary computing basics, data storage and resources for networking, end users can substantially negotiate the various opportunities and resources to acquire present-day facilities and applications. Consequently, "Fog as a Service (FaaS)" [11] has reflected to be an invigorating fortuity, which labours a fog service provider by assembling a series of fogs at innumerable topographical locations to manifest services from vertical point solutions. Thereby, fog computing is adjudged as a utility prototype, wherein statistics is cumulated, organized and scrutinized enclosed in the network, rather than in a centralized cloud.

3. Architecture of Fog-Enabled IoT

Fog computing pertains with the augmented arithmetical values of coupled mechanisms and various emanating implementations in IoT by insightfully mobilizing and managing computing, storage and organizational assets allocated alongside the extremities of network [12] as described in Fig.2 of the next section. By exploiting the resources, fog computing proposes a sequence of extraordinary operations, functions and services, such as hierarchical study of data, percipient deployment in functioning of amenities like the traffic lights, disaster response, parking pre-arrangements, etc. It also aids to intently solve defiance's of hibernation; restricted frequencies and constrained accumulations of IoT smart gadgets

The Problem Statement

The multinational companies around the globe spend humongous aggregates of capital on remunerations for the computer veterans in assorted fields aiming to fabricate direct products or technologies encapsulated into concrete and substantial things to usher operationally streamlined structuring and methodology in objects and framework, via the vision of Internet of Things. Various researchers are consistently persuading on the architectures, compatibility, soundness, reliability, and security contrivances during data transferal among IoT devices. A noteworthy characteristic being the unassailability of devices and statistical data transmission primarily demands developing high level, standard and reliable software mechanisms. A diversified realm of international laws being customized aims to benefit the field of information technology.

Large volumes of data are precipitated by divergent entities assembling and connecting with the Internet. The advantages are innumerous; however, issues of computational proficiency scarcity of storage, lack of momentum and speed capacity, and various other concerns related to security arise as the couple of confrontations and challenges faced by the upcoming technologies. In accordance to strive and decipher these relevant issues, a modern-day technology which denominated in the guise of "Fog Computing" has been successively attaining grip in the market these days. Predominantly, the ubiquitous sanctioning of the Fog Computing paradigm necessitates the enlargement and expansion of modern network constitutions and middleware platforms. Fog Computing is advocated to empower computing and quantifying of the data directly adjacent to the devices that induce, foster, trigger and entail data processing, with the purpose for delivering new applications for billions of interconnected devices.

Fog Computing is defined as a disseminated computing framework or infrastructure by which the applications and assistances are controlled either at the network edge or in a remote data center cloud. The Fog paradigm serves with the major advantage by bringing partial and fragmented computational storage ethically at the extremity of the network; which facilitates to diminish the intrinsic latency and the congestion hold-ups affecting Internet bandwidth [13].

4. Fog-Enabled IoT Distributed Computing Model

Fogs function by periodically forwarding summaries of data to the cloud, in case, if imperishable repository and perusal are required globally. Henceforth, it is said that fog computing is not an opponent of the cloud in IoT. On the contradictory, it is visualized as a perfect commendation for massive volumes where cloud computing is found to be inadequate and restricted in satisfying some part of demands exceptionally. Fog computing can broaden and supplement an assortment of IoT approaches under the layout of fog enabled IoT implementations. The adaptive and methodical concatenation of fog computing and IoT amplifies web-work connectivity

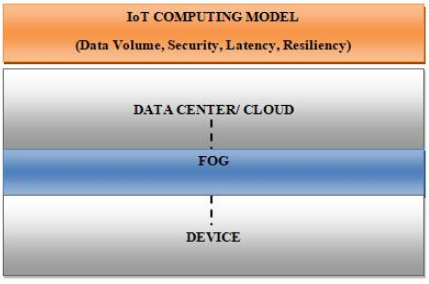

Figure 2: Fog-Enabled IoT Distributed Computing Model

and potentiality to nearly support the global, unlimited, and pervasive IoT applications. With the webbing documentations at the network's edge, fogs circumscribe IoT services and data stockpiles as a representative of the intermediates, annexing the superior cloud layers and the button device layering, as given in Fig. 2 [13].

4.1 The Cloud

The cloud facilitates its services by amplifying miscellaneous IoT approaches for gadgets with practically unrestrained storehouse and computational assets. The data handling epicenters hold the accountability for rendering externalized data storage assistance to gadgets and reckoning competences for modelling and inspection of data. The application servers cope up with the accessing of invocations from devices and deploying a productive network which extends to propound rich and concentrated IoT services [14, 15].

4.2 The Fog

This layer is stated to be a nexus of fogs, which constitutes a colossal of cell base stations both small-scale/large-scale and Wi-Fi hotspots. These hold the potential to assemble network associations linking devices and cloud servers. In addition to this, the layer is proficient to engage various computing and warehouse having resources which aim to allocate localized services and IoT applications. Instinctively, fogs are amplified from conventional and foundational base stations with computational competences which reinforce data preliminary practices having economical latency facilities [16, 17].

4.3 The Devices

The cloud connects an extensive and substantial number of devices for delivering a diverse range of IoT applications. The devices which are technologically advanced hold the potential to procure the relevant and stimulated data from the domain, yield fabricated data to cloud servers and make avenues towards various latency-sensitive services [18].

5. Issues of Fog Computing

Notwithstanding that, even though, the paradigm of Fog is fascinating; but the fact which holds foremost criticality is the inscription and to apprehend the divergent concerns that arise with the usage and deployment of the Fog Computing approach [19]. In data-exhaustive IoT, fogs take advantage of their artifices to accomplish the duties of prior treatment of the data for latency curtailment and ameliorating the throughput of the network. With the requisites and intentions to attain the objectives of Fog Computing, there arises a compulsion to discern the divergent situations and issues that advance with administering the implementation of the Fog Computing paradigm. Listing a few of these arguments would state the following:

5.1 Fog Network

One of the ingredients which is termed to be pivotal for this computing implementation to be magnetic and vigorous is the network itself which is the considered to be the nucleus fastening all the disparate and miscellaneous constituents (devices and gadgets) gaining access to enumerate resources. Various issues, likewise, the attainment of scalability in the network and cost reduction can be managed by deploying fog networks [20, 21].

5.2 Quality of Service (QoS)

QoS is termed to be a very predominant estimate of the quality of provisioning services in computing network of the fog. This parameter is engineered by measuring four metrics namely connectivity, capacity, reliability and delay continuously [22].

5.3 Interface and Programming Model

For the reason that the available assets in the computing network of a fog are accessible by the use of virtual lattices, there arises an obligation for programming models to be resilient and in support for the interfacing to be effective and dynamic. The points which are in-vogue and need to be deliberated pertaining to achieving an application-centric computing have a proficient fortune in Fog Computing and aim to impart framework where components in the computing environment will be more cognizant with the application authorizing contrasting categories of optimizations [23, 24].

5.4 Computation Offloading

The computational effectiveness can be enhanced by making extensions in the lifetime of the battery or by enabling of a disseminated memory allocation on computational tasks which are comprehensive in nature [25].

5.5 Provisioning and Resource Management

With the end nodes making progressions, the applications which are conscious of contingencies is jeopardized. The reason being the dynamism invoked in the rhythm of various metrics for instance, the bandwidth, storage, latency, etc. [26, 27, 28]. Resource sharing is described to be a key solution and hallmark that requires to be considered cautiously in variegated resource environments to vanquish the contrasting provocations summoned about by Fog Computing [29, 30].

5.6 Privacy and Security

Whilst the efforts constantly devoted and safeguarded by numerous scrutinizers on security arguments with reference to Cloud computing environment, there still remains scattered arbitrations and attempts to be committed to fog computing [31]. The implementation of personalized frameworks on intrusion detection systems can be exploited in geographically diffused fog computing environments to unearth the malicious activities which seem to be mistrusted such as denial of service attacks (DoS), port contemplations, etc [32]. There arises an obligation to inspect the security subjects in thickness of both the hardware layer and the software layer.

6. Challenges of Fog Computing

The paradigm of fog computing manifolds disparate challenges. The utmost and considerable pitfall of the architecture is that it escalates the intricacies of the divulgence of the network, adding an undeniable proportion of overhead expenses in business tenancy—levelling both directly and indirectly; benefitting the security and privacy but impacting the maintenance and probability aspects to great extents [33].It is needed that the security and privacy should be undertaken in each and every thickness of layers while sketching the blueprint of the system [34]. The archaic solutions which operated by the end user having an isolated tapered extremity of failure with rationalized attempts to distinguish, renovate and prolong the unrealized issues in the computing architecture. But with the widespread of the network on a massive scale the computational load, effort and responsibility, enlarges the strain on the intact Fog Computing process [35, 36]. Fog is hence considered to be another layer of a distributed webbing environment having familiarity with cloud computing and the Internet of Things [37]. Researchers and professionals strive in instituting the cue postulates that are under compulsion and mentor in the designing and implementation of Cloud and Fog Computing [38]. The following ethics are nucleus to platform the delineating of the computing applications:

i. Designs need to opine the fundamental conception and ideologies of reliability, availability and serviceability [39]. The constitution of cloud services should be such that it is invariably approachable to the end-users. Nevertheless, the requirement for universal comprehensibility of Fog applications promotes the hike in such applications to have countless scores of security concerns and challenges [40].
ii. The decision-making executed more strategically, tactfully and with intrigued organization renders agile applications that are elemental in the metamorphosis of data and discernment. Cloud resources should be agile such that it sanctions customizations in the configurations of the service models on any occasion of justified tailoring in the requisites of the customers.
iii. Development of extensive Cloud-accredited computational procedures observing autonomy at all levels [41].
iv. Virtualization and multi-tenancy should be facilitated which promote the users to ingress the Cloud services concurrently; unaccompanied by the curtailment in the degrees of the provisions.
v. Promoting flexibility, autonomy and examination of the factual value of data [42].
vi. Unambiguous to needs of categorization and consideration of all captivated ethics and assessments of privacy. This feature is needed as with the change and innovations there are contemporary services and applications that unfold every day. Cloud services should

distinguish exorbitant degrees of extensibility and scalability.

vii. Another essential provocation in accelerating Fog Computing is erecting the obligatory measure of interoperability to reinforce the retrieval of Fog Computing resources.

viii. Data management in fog computing comes forth to be a significant dispute where the cloud's expansive "centralized storage" conceptualization is superseded by the fog's disseminated storage space into many nodes. Pedagogies to coherently accumulate and obtain the statistics, summon the statistics with moderate latency, stockpiling of the encrypted data and still bring into fruition the energy consumption are the present-day research issues in Fog.

ix. Maintaining and executing data consistency in the fog environment, whilst the data hoarding and fetching of data is also an open area of interrogation for the practitioners in this domain. The devices which are of arbitrary and random nature in the fog architecture find it very strenuous to interchange information due to the encryption and inflexible stratagems on privacy.

One elucidation concerned with engineering the interoperability in Fog Computing background is to necessitate for an open architecture which will not be contingent on the manufacturing and prototype of technical knowledge and innovation accessing the computing environment. An open infrastructure will remarkably minimize the quotations to expand the fog applications and dispense a recurrent platform alongside which the applications will be flourished, increasing penetration and adoption of the technology; ultimately giving a boost to the quality and innovation of Fog Computing criterion [43, 44].

The complications of fog computing can therefore, be dominated by captivating the issues of efficiency and effectiveness incessantly. The vital postulates for acquiring the security management dynamism in loud computing environments is safeguarding of rugged and robust identity management while handling the various processing mechanisms.

7. Security of Blockchain

The block chain technology holds accountability for providing a secure proposal that addresses the above concerns for edge architectures. Blockchain accredit to forms of software architectures which are disseminated and operate in consensus on shared state for the data which are decentralized and transactional in nature and can be initiated across a telegraph of duplicitous contributors – as found in the case of the edge clouds. This methodology abstains from depending on central trusted integration points, which immediately become single purposes of disappointment and failure. Edge platforms based on blockchain can exploit basic blockchain properties, for example, information immutability, integrity, fair and reasonable access, transparency, and non-repudiation of exchanges [45]. The key point is to oversee and believe lightweight edge bunches with low computational abilities and restricted availability locally. Blockchain advances can be applied to identity management, information provenance, and processing of different exchanges.

Security Requirements and Blockchain Principles

Blockchain innovation is an answer for mistrustful situations that are deficient in a central authority or confided in outsider. Numerous security-related issues can be tended to utilizing the decentralized, self-ruling, and confided in capacities of blockchains. Also, blockchains are carefully designed, dispersed and shared information bases where all participants/ members can add and read exchanges (transactions) yet nobody has full authority over it. Each additional exchange is digitally signed and time-stamped. This implies all operations can be followed back and their provenance can be resolved [45]. The security model actualized by blockchains guarantees information integrity utilizing consensus-driven components to empower the verification of the apparent multitude of exchanges in the organization, which makes all records effectively auditable. This is especially significant since it permits following all sources of uncertain exchanges in the organization (e.g., vulnerable IoT gadgets) [46]. A blockchain can likewise fortify the security of edge components regarding identity management, manage access control and forestall information control and manipulation. The standards of blockchains can be summed up as follows:

i. A transaction is a signed snippet of data made by a node in the network, which is then transmitted to the rest of the network. The transactions are digitally signed to keep up trustworthiness and uphold non-repudiation.

ii. A block is an assortment of transactions that are added to the chain. A newly made block is advocated by checking the legitimacy of all transactions contained inside.

iii. A blockchain is a rundown of all the created and approved blocks that make up the network organization. The chain is shared between all the hubs in the network organization. Each recently made and approved block is connected to the past block in the chain with a hash value produced by applying a hashing calculation algorithm

over its content. This permits the chain to keep up non-repudiation.

iv. Public keys go about as addresses. Members in the network organization utilize their private keys to sign their transactions

v. A block is attached to the current blockchain utilizing a particular agreement technique and separate co-ordination convention. Consensus is driven by gathered personal circumstances [46].

8. IoT and Blockchain Integration

The IoT is changing and streamlining manual cycles to make them part of the computerized era, acquiring volumes of information that presents knowledge at incomprehensible levels. This information is encouraging the advancement of smart applications, for example, the improvement of the administration and the personal satisfaction of residents through the digitization of provisions in the urban areas. Throughout the most recent couple of years, distributed computing innovations have added to giving the IoT with the vital usefulness to break down and measure data and transform it into real-time activities and information. This remarkable development in the IoT has opened up new network openings, for example, instruments to access and share data. The open information paradigm is the flagship in these resourcefulness activities. Nonetheless, one of the most significant weaknesses of these activities, as has happened in numerous situations, is the absence of certainty. Centralized models like the one utilized in distributed computing have fundamentally added to the advancement of IoT. In any case, viewing information transparency and straightforwardness they go about as black boxes and network members do not have an unambiguous visualization from of where and how the data they provide will be utilized. The combination of promising innovations like IoT and distributed computing has demonstrated to be significant. Similarly, we recognize the tremendous capability of blockchain in transfiguring the IoT.

Blockchain can enhance the IoT by offering a confided in sharing assistance, where data is dependable and can be recognizable. Information sources can be recognized anytime and information stays unalterable overtime, expanding its security. In the situations where the IoT data ought to be safely shared between numerous members this incorporation would speak to a key upheaval. For example, a comprehensive discernibility in numerous food items is a key viewpoint to guarantee food safety and sanitation. Food detectability could require the inclusion of numerous members: fabricating, feeding, treatment, conveyance, etc. An information spill in any aspect of the chain could prompt misrepresentation and hinder the cycles of the quest for infection which can truly influence resident's lives and acquire tremendous financial expenses to organizations, segments and nations on account of a food borne flare-up. A superior control in these territories would increase food sanitation, improving the information sharing among participants and decreasing the search time on account of a food borne outbreak, which can spare human lives. Also, in different zones, for example, smart urban areas and savvy vehicles, sharing solid and reliable information could support the consideration of new participants in the environments and add to improve their services and their selection. Consequently, the utilization of blockchain can supplement the IoT with dependable and secure data. This has begun to be perceived as referenced in, where blockchain innovation is recognized as the way to understand scalability, versatility, protection, and dependability issues identified with the IoT worldview.

From our perspective IoT can incredibly profit from the functionality gave by blockchain and will assist with further advancing current IoT technologies. Another angle to be taken in to account is identified with the IoT associations, i.e., the correspondence between the underlying IoT infrastructures. When co-ordinating blockchain, it should be chosen where these associations will happen; inside the IoT, a hybrid design including IoT and blockchain, or through blockchain. Fog computing has additionally reformed the IoT with the inclusion of a new layer between cloud computing and IoT gadgets and could likewise encourage this co-ordination. There are three proposed structures to construct the IoT network with the blockchains. Highlights of the specific application are the characterizing components to utilize which to where. We should examine them as stated below:

8.1 IoT–IoT INTEGRATION

This methodology could be the quickest one when concerning latency and security since it can work disconnected. IoT gadgets must be alternative to verbalize with one another, which normally includes innovation and routing mechanisms. Just a piece of IoT information is put away in blockchain though the IoT communications occur without utilizing the blockchain as shown in Fig. 3. This methodology would be helpful in situations with reliable IoT information where the IoT communications are occurring with low latency.

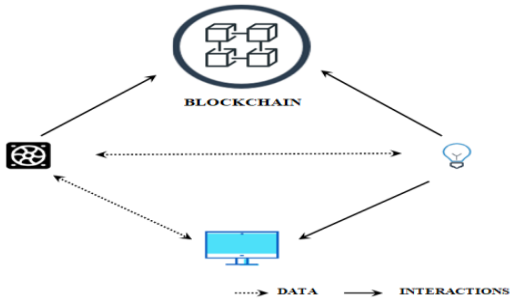

Figure 2: IoT-IoT Application

8.2 IoT-BLOCKCHAIN INTEGRATION

In this methodology all the communications experience blockchain, empowering a permanent record of associations as in Fig. 4. This methodology guarantees that all the chosen communications are recognizable as their subtleties can be questioned in the blockchain, and in addition it builds the autonomy of IoT gadgets. IoT applications that plan to exchange or lease, for example, Slock; it can use this way to recommend their assistances.

Even so, recording all the communications in blockchain would include an expansion in transfer speed and information, which is one of the notable difficulties in blockchain. Then again, all IoT information related with these exchanges ought to likewise be stored in blockchain.

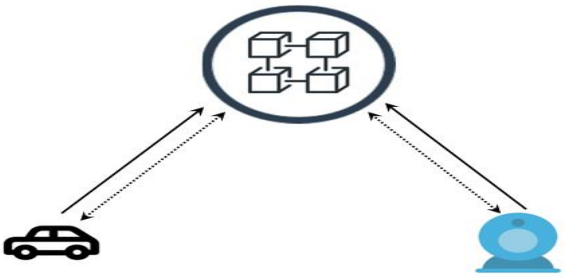

Figure 4: IoT-Blockchain Integration

8.3 HYBRID APPROACH

In conclusion, a hybrid plan where only aspect of the connections and information transpire in the blockchain and the rest are straightforwardly shared between the IoT gadgets as given below in Fig.5. One of the difficulties in this methodology is picking which exchanges ought to experience the blockchain and giving the best approach to choose this in run time. An ideal synchronization of this methodology would be the most ideal approach to incorporate the two innovations since it exercises the advantages of blockchain and the advantages of real-time IoT associations. In this methodology fog computing could become an integral factor and even cloud computing, to supplement the constraints of blockchain and the IoT. For instance, fog computing includes less computationally restricted gadgets, for example, gateways and it is a potential spot where mining can happen similarly as different initiatives that exploit IoT gadgets.

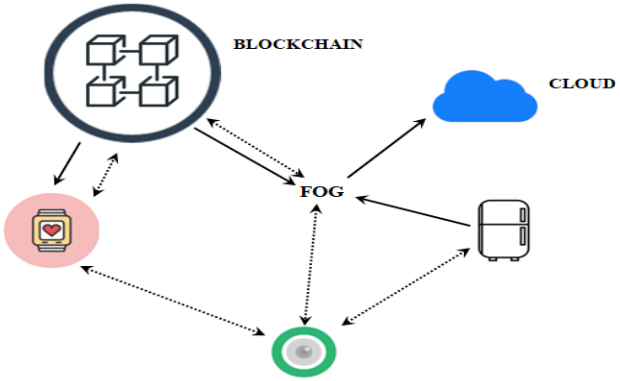

Figure 5: Hybrid Integration

9. Future Research Direction

Fog computing anticipates prolific probabilities for fabricating modern applications and services that cannot be simply propped by the currently accessible quantifying communication models. The computing paradigm of cloud is maturing and sophisticating rapidly. The upcoming focus is on Fog computing. There are pivotal use cases demanding the fog capability. The forthwith applications, analytics and services stipulate advanced and revolutionized Fog background. The Quality of Service (QoS) and Quality of Experience (QoE) attributes subject to fulfilment suitably to haul the concept of fog moderately [47]. The faster multiplication of fog environments is the need of the hour.

Multitudes of recently developed and advanced Fog-based security resources will inevitably master and succour to tackle and confront multitudinous challenges being faced directly helping to procure and tighten the Internet of Things [48]. The supplemental rationale which promotes Fog to outshine subsequently in the due course is that data suffers deprivation of its estimates when it cannot be probed and audited impulsively. The foundation of fog computing and its infrastructure works by capturing all sorts of data immediately and the process includes subjecting the data to a classified range of investigations with the intent of extraction and exposing of insights

which require immediate actions to be accomplished. The Fog analytics serves as an eminent supporter of multiple use cases covering trademark verticals resembling fields of lubrications and gas fabrication, banks and merchants, etc. Security cameras, smart phones, sensor-attached physical assets, digitized entities, drones, robots, thermostats, advanced cars and IP televisions are being boundlessly being deployed in conventional environments. These induce to generate a good deal of operational and serviceable data to incite on. Thus, the quantity of IoT statistics gets greater day by day. Also, data monetization is another intended discipline being scouted by various industry verticals. The fast pacing size, purview, swiftness and anatomy of statistics convey forward prodigious opportunities and prospects for the technological professionals. Organizations are in the conception to reckon at Fog computing as the response [49]. We also through this review paper identified some limitations and have examined concerns that require further work, for example, the security viewpoint where we investigated blockchain innovations for provenance and identity management that needs more consideration. We have talked about blockchain innovation for provenance management and other security worries as a potential solution, however here more execution and observational assessment works are to be acted later on.

Considerations

Big data has contemporarily transformed into one of the sensitive and burning subject in fields of both academic circles and trade predominantly owing to its range, amplitudes and intricacy. The Fog paradigm furnishes diminished latency and perspective cognizance; for the reason that of the restraining of Fog nodes and substructures perpendicularly secluded latency-sentient functions by advancements in delivering of ubiquitous, adaptable, layered and federated network organization correspondence. Additionally, the Fogging architecture operates on superfluous amalgamations of end-user clients or near-organisation edging devices to effectuate considerable amounts of communication, jurisdiction, configuration, computations and services of governance. It is a concept that broadens Cloud computing provisions and resources to the periphery of the network association. The discriminating characteristic actualizing that the cloud environment may be topographically prolonged from the organisation and habitually unaware where the Cloud-based services actually are inherent in, and hinging profoundly on the largely-scaled Internet bandwidths; whereas, the provisions in the Fog paradigm are nearer to the end-users with intense geographical diffusions, exceptional support and maintenance for mobility.

10. Conclusion

The irresistible and captivating environment of Fog computing will culminate in the unfolding of advanced big business representations, henceforth assisting the organizations to flourish supplementary methodically and rapidly. As a consequence of which new marketers and industries will approach imminently with fresh benefactions and new architectural viewpoints to networking. One exhilarated phenomenon of evolution and progressions is Fog-as-a-Service (FaaS) [50] where a Fog service contributor establishes unified and coordinated fog nodes to shield a territorial area of service. This, sequentially, will be helpful in imparting extended and favourable opportunities for actualizing contemporary and advanced breakthrough applications and resources that the ongoing host-based and Cloud-based manifesto are unable to develop comfortably and efficiently. This can be illustrated by the attribute evidenced that the Fog-based security services is capable to detail many challenges and other facets that are lately being confronted in the IoT environment [51, 52]. The broadcasting of 5G technologies, enlargement of smart city applications and assembling of the diffused and dispersed computing environments with implanted ambient wittedness will assist in innovation of the quality of life [53, 54]. Fog Computing-based systems are transforming to become cardinal and dominant in day-to-day lives. It is reasonably and thoroughly transparent from the above deliberations that Fog Computing will, in future, be infinite, prevalent and penetrating covering various disciplines, likewise social and commercial [55,56]. This would even benefit the earthen things directly and is more probably to fetch excessive computation capabilities with pre-eminence, through the incorporation of intrinsic electronic gadgets and embedded processing potentiality. The exquisiteness of this know-how technology is that all smart devices, including smart phones, already enchant this computational technology. All the IT-related organizations are blossoming IoT products and resources to Fog computing hardware, software, and networking interoperability [57, 58]. Nevertheless, practitioners still have much effort to deploy on the fundamentals of Fogging and its federated applications to prosper the conventional as well as stereotypical Fogging prototypes and architectures.

References

[1] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7):2013, 1645–1660.

[2] Chang, S.N. Srirama, and R. Buyya. Mobile cloud business process management system for the Internet of Things: A survey. ACM Computing Surveys, 49(4): 70:1–70:42, December 2016.

[3] Afshan Zameer, Pawan Kumar Chaurasia, (2018): "A Review on Crypto-Currency", International Journal of Computer Science and Mobile Applications, ISSN (online): 2321-8363 Vol.6, Issue. 1, January- 2018, pg. 95-100.

[4] M. Chiang and T. Zhang, Fog and IoT: An overview of research opportunities. IEEE Internet of Things Journal, 3(6):2016, 854−864.

[5] H.P. Sajjad, K. Danniswara, A. Al-Shishtawy and V. Vlassov. Span Edge: Towards unifying stream processing over central and near-the-edge datacenters. In Proceedings of the IEEE/ACM Symposium on Edge Computing (SEC, IEEE, 2016.), pp. 168–178.

[6] M. Satyanarayanan, P. Bahl, R. Caceres and N. Davies. The Case forVM-Based Cloudlets in Mobile Computing, IEEE Pervasive Computing, 8(4): 14–23, 2009.

[7] Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, 2015, vol. 17, no. 4, pp. 2347–2376.

[8] Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: a survey," Future Generation Computer Systems, 2016, vol. 56, pp. 684–700.

[9] C. W. Tsai, C.-F. Lai, M.-C. Chiang, L. T. Yang et al., "Data mining for internet of things: A survey." IEEE Communications Surveys and Tutorials, 2014, vol. 16, no. 1, pp. 77–97.

[10] J. Ni, Y. Yu, Y. Mu, and Q. Xia, "On the security of an efficient dynamic auditing protocol in cloud storage," IEEE Transactions on Parallel and Distributed Systems, 2014, vol. 25, no. 10, pp.2760–2761.

[11] F. Jalali, K. Hinton, R. Ayre, T. Alpcan, and R. S. Tucker, "Fog computing may help to save energy in cloud computing," IEEE Journal on Selected Areas in Communications, 2016, Vol. 34, No. 5, pp. 1728–1739.

[12] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proc. of MCC, 2012, pp. 13–16.

[13] Fog computing: Fog and Cloud along the Cloud-to-Thing continuumwww.i-scoop.eu.

[14] Fog Computing: A New IoT Architecture? RTInsightswww.rtinsights.com.

[15] P. Sharma and Pawan K. Chaurasia, "Proposed Algorithm for Secured Transaction using 3-Tier Architecture", International Journal of Computer Sciences and Engineering, Vol. 6, No. 6, pp. 316-321, 2018. Available: 10.26438/ijcse/v6i6.316321.

[16] P. Hu, H. Ning, T. Qiu, Y. Zhang, and X. Luo, "Fog computing based face identification and resolution scheme in internet of things," IEEE transactions on industrial informatics,2017, Vol. 13, no. 4, pp. 1910–1920.

[17] P. Garcia Lopez, A. Montresor, D. Epema, A. Datta, T. Higashino, A. Iamnitchi, M. Barcellos,P. Felber, and E. Riviere, "Edge-centric computing: Vision and challenges," ACM SIGCOMM Computer Communication Review,2015, vol. 45, no. 5, pp. 37–42.

[18] S. Singh, N. Yadav and Pawan K. Chaurasia, "A Review on Cyber Physical System Attacks: Issues and Challenges," 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2020, pp. 1133-1138, doi: 10.1109/ICCSP48568.2020.9182452.

[19] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," IEEE Internet of Things Journal, vol. 3, no. 6, pp. 854–864, 2016.

[20] M. Tao, K. Ota, and M. Dong, "Foud: integrating fog and cloud for 5g-enabled v2g networks," IEEE Network, vol. 31, no. 2, pp. 8–13, 2017.

[21] J. Ni, K. Zhang, X. Lin, Y. Yu, and X. Shen, "Cloud-based privacy-preserving parking navigation through vehicular communications," in Proc. of Securecomm, 2016, pp. 85–103.

[22] J. Ni, A. Zhang, X. Lin, and X. Shen, "Security, privacy, and fairness in fog-based vehicular crowd sensing," IEEE Communications Magazine, 2017, Vol. 55, no. 6, pp. 146–152.

[23] J. Ni, K. Zhang, K. Alharbi, X. Lin, N. Zhang, and X. Shen, "Differentially private smart metering with fault tolerance and range-based filtering," IEEE Transactions on Smart Grid,2017, Vol. 8, no. 5, pp. 2483–2493.

[24] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for internet of things applications: Challenges and solutions," IEEE Communications Surveys & Tutorials, 2017, vol. 20, no. 1, pp. 601–628.

[25] Cearley DW (2010) Cloud computing: key initiative overview. Gartner Report, 2010

[26] Mahmood Z (2011) In: Mahmood Z, Hill R (eds) Cloud computing for enterprise architectures. Springer, Berlin.

[27] Bonomi F, Milito R, Zhu J, Addepalli S (2012) Fog computing and its role in the internet of things. In: Proceedings of the first edition of the MCC workshop on mobile cloud computing, MCC' 12, ACM, 2012, pp 13–16.

[28] Cisco (2013) Fog computing, ecosystem, architecture and applications. Cisco Report RFP-2013-078.

[29] Greenfield D (2016) Fog computing vs. edge computing: what's the difference? https://www.automationworld.com/Fog-computing-vs-edge-computing-whats-difference.

[30] OPTO-22 (2018) Fog computing vs. edge computing. http://info.opto22.com/Fog-vs-edgecomputing.

[31] Shariffdeen R (2017) Fog computing vs. edge computing. https://medium.com/@rshariffdeen/edge-computing-vs-Fog-computing-5b23d6bb049d.

[32] Shah H (2017) Edge computing and fog computing for enterprise IoT. https://www.simform.com/iot-edge-Fog-computing/.

[33] Open Fog (2017) Open Fog reference architecture for fog

computing.Fogconsortium.org/wpcontent/uploads/OpenFog_Reference_Architecture_2_09_17-FINAL-1.

[34] McKendrick J (2016) Fog computing: a new IoT architecture? https://www.rtinsights.com/ what-is-Fog-computing-open-consortium/.

[35] Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, 2015, vol. 17, no. 4, pp. 2347–2376.

[36] Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: a survey," Future Generation Computer Systems, 2016, vol. 56, pp. 684–700.

[37] C.-W. Tsai, C.-F. Lai, M.-C. Chiang, L. T. Yang et al., "Data mining for internet of things: A survey." IEEE Communications Surveys and Tutorials, 2014, vol. 16, no. 1, pp. 77–97.

[38] J. Ni, Y. Yu, Y. Mu, and Q. Xia, "On the security of an efficient dynamic auditing protocol in cloud storage," IEEE Transactions on Parallel and Distributed Systems, 2014, vol. 25, no. 10, pp.2760–2761.

[39] F. Jalali, K. Hinton, R. Ayre, T. Alpcan, and R. S. Tucker, "Fog computing may help to save energy in cloud computing," IEEE Journal on Selected Areas in Communications,2016, vol. 34, no. 5, pp. 1728–1739.

[40] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proc. of MCC, 2012, pp. 13–16.

[41] Schubert L, Jeffery K (2012) Advances in clouds expert group report public version 1.0 research in future cloud computing. In: Schubert L, Jeffery K, Research in future cloud computing.

[42] Ukil A, Jana D, De Sarkar A (2013) A security framework in cloud computing infrastructure. Int. J Netw Secur Appl (IJNSA) 5(5). https://doi.org/10.5121/ijnsa.2013.550211.

[43] Stanton B, Theofanos M, Joshi KP (2015) Framework for cloud usability NIST special publication 500–316. http://dx.doi.org/10.6028/NIST.SP.500-316. Accessed 3 May 2017.

[44] Yi S, Li C, Li Q (2012) A survey of fog computing: concepts, applications andissues.http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.702.7773&rep=rep1&type=pdf. Accessed 26 Oct 2017 of life in the Grid. Sci. Program 13(4):265–275.

[45] Nurmi D, Wolski R et al (2009) the eucalyptus open-source cloud-computing system. In: Proceeding of 9th IEEE/ACM international symposium on cluster computing and the grid.

[46] Barham P, Dragovic B, Hand SK, Harris T, Ho A, Neugebauery R et al (2003) Xen and art of virtualisation. http://www.cl.cam.ac.uk/research/srg/netos/papers/2003-xensosp.pdf. Accessed 26 Oct 2017.

[47] Vaquero LM, Rodero-Merino L (2014) Finding your way in the fog: towards a comprehensive definition of fog computing. ACM SIGCOMM Comput Commun Rev 44(5):27.

[48] Pahl, N. El Ioini, and S. Helmer. A decision framework for blockchain platforms for IoT and edge computing. International Conference on Internet of Things, Big Data and Security, 2018.

[49] Dorri, S. Salil Kanhere, and R. Jurdak. Towards an Optimized BlockChain for IoT, Intl Conf on IoT Design and Implementation, 2017.

[50] N. Kshetri. Can Blockchain Strengthen the Internet of Things? IT Professional, 2017, 19(4): 68–72.

[51] Kitanov S, Janevski T (2016) State of the art: fog computing for 5G networks, 24th telecommunications forum TELFOR, 2016.

[52] Vaquero LM, Rodero-Merino L, Gradiant Vigo L (2014) Finding your way in the fog: towards a comprehensive definition of fog computing. ACM SIGCOMM Comput Commun Rev 44:27–32.

[53] Ai Y, Peng M, Zhang K (2017) Edge computing technologies for internet of things: a primer. Digit Commun Netw OpenFog Consortium Architecture Working Group (2017) OpenFog reference architecture for fog computing.

[54] Bonomi F, Milito R, Zhu J, Addepalli S (2012) Fog computing and its role in the internet of things. In: Proceedings of the first edition of the MCC workshop on Mobile Cloud computing—MCC '12, 2014, P.13. ACM Press, New York, NY, USA.

[55] Banafa A What is fog computing?https://www.ibm.com/blogs/Cloud-computing/2014/08/fog-computing/.

[56] Dastjerdi AV, Buyya R (2016) Fog Computing: helping the internet of things realize it's potential. Computer 49(8):112–116.

[57] Luan TH, Gao L, Li Z, Xiang Y, Sun L, 2015, Fog Computing: focusing on mobile users at the edge. CoRR, vol. abs/1502.01815.

[58] Stojmenovic I, Wen S (2014) The Fog Computing paradigm: scenarios and security issues. In: 2014 federated conference on FedCSIS. IEEE.

[59] Shahid MA, Sharif M, 2015, Cloud computing security models, architectures, issues and challenges: a survey. Smart Comput Rev 5:602–616.

AUTHOR'S PROFILE

Srishti Garg is pursuing M.Tech. (Software Engineering) with Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh in the Department of Information Technology. She received her Bachelor Degree in Computer Science and Engineering from Uttar Pradesh Technical University, Lucknow, Uttar Pradesh, India in 2014. Her research areas include Cloud Computing, Machine Translation, Natural Language Processing and Machine Learning.

Pawan Kumar Chaurasia is working as an Associate Professor and Head with Mahatma Gandhi Central University, Motihari, Bihar in the Department of Computer Science and Information Technology. He was working as an Assistant Professor in the

Department of Information Technology, Babasaheb Bhimrao Ambedkar University, (A Central University), Lucknow, India prior to this. He has published more than 30 International Journal papers, prsented more than 20 research papers and delivered more than 10 lectures. His research area includes Software Reliability, Software Quality, Software Testing, Machine Learning and IoT.