Blockchain for Edge of Things: Applications, Opportunities, and Challenges

Thippa Reddy Gadekallu, Quoc-Viet Pham, Dinh C. Nguyen, Praveen Kumar Reddy Maddikunta,
N Deepa, Prabadevi B, Pubudu N. Pathirana, Jun Zhao, and Won-Joo Hwang

***Abstract*—In recent years, blockchain networks have attracted significant attention in many research areas beyond cryptocurrency, one of them being the Edge of Things (EoT) that is enabled by the combination of edge computing and the Internet of Things (IoT). In this context, blockchain networks enabled with unique features such as decentralization, immutability, and traceability, have the potential to reshape and transform the conventional EoT systems with higher security levels. Particularly, the convergence of blockchain and EoT leads to a new paradigm, called *BEoT* that has been regarded as a promising enabler for future services and applications. In this paper, we present a state-of-the-art review of recent developments in BEoT technology and discover its great opportunities in many application domains. We start our survey by providing an updated introduction to blockchain and EoT along with their recent advances. Subsequently, we discuss the use of BEoT in a wide range of industrial applications, from smart transportation, smart city, smart healthcare to smart home and smart grid. Security challenges in BEoT paradigm are also discussed and analyzed, with some key services such as access authentication, data privacy preservation, attack detection, and trust management. Finally, some key research challenges and future directions are also highlighted to instigate further research in this promising area.**

***Index Terms*—Blockchain, Edge Computing, Internet of Things, Edge of Things, Security, Industrial Applications.**

I. Introduction

In recent years, we have witnessed rapid advances in Internet of Things (IoT) empowered by the proliferation of mobile devices such as smartphones, laptops, sensors, wearables, etc. It is predicted that by 2030, the number of connected IoT devices surpasses 500 million [1]. This tremendous expansion of IoT is expected to create numerous applications and services across different application domains, from entertainment industry to mobile games and surveillance [2]–[4]. Such IoT applications often require high computing resources to handle massive data generated from sensor devices with latency requirements to provide time-sensitive customer services, like, transportation and smart healthcare. Cloud computing can support IoT devices in solving computation tasks, but high transmission latency remains a challenge due to long distance from the users. Edge computing has been recently proposed to support IoT with the creation of *Edge of Things* (EoT) networks, by migrating computing and storage to the edge of the network, e.g., access points or base stations of radio access networks [5]–[7]. In this regard, the computational burden posed on resource-constrained IoT sensors can be eliminated and the communication overhead is significantly reduced while providing better computing experience for the users. Therefore, EoT possess the ability to support location-aware distributed IoT applications to facilitate time-sensitive service delivery with reduced computation complexities [8].

The distributed nature of EoT introduces new security and privacy challenges. The migration of large-scale computing and storage services to the edge creates the possibility of security threats and helps in controlling the network or prevent attacks on the resources at edge nodes [9], [10]. Moreover, uploading data to the network edge also raises critical data privacy concerns such as data breaches, data attacks and data modifications. Blockchain, a disruptive technology that emerged in recent years, has been regarded as a promising solution to solve security and privacy issues in edge computing networks as well as empower the next generations of EoT technology [11]–[13]. In particular, the convergence of blockchain and EoT creates a novel paradigm called *BEoT*, which reshapes and transforms the conventional edge-IoT networks to enable new industrial and customer applications and services [14], [15]. For example, BEoT has been used to provide secure smart city services such as reliable vehicular management and low-latency traffic control [16]. Further, BEoT has promoted smart healthcare analytics and IoT medical processing due to the large-scale computing and communication features of EoT and security features of blockchain [17]. The convergence of these emerging technologies is potentially a key enabler for future services and applications.

A. BEoT Architecture

In this article, we propose a novel BEoT architecture that is enabled by the use of blockchain in EoT, as illustrated in Fig. 1. The proposed architecture consists of three main entities; IoT, edge computing, blockchain, along with industrial applications and BEoT security services.

Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, N Deepa, Prabadevi B are with the School of Information Technology and Engineering, Vellore Institute of Technology, Tamilnadu, India (e-mail: {thippareddy.g, praveenkumarreddy, deepa.rajesh, prabadevi.b}@vit.ac.in).

Quoc-Viet Pham (corresponding author) is with the Korean Southeast Center for the 4th Industrial Revolution Leader Education, Pusan National University, Busan 46241, Korea (e-mail: vietpq@pusan.ac.kr).

Dinh C. Nguyen and Pubudu N. Pathirana are with the School of Engineering, Deakin University, Waurn Ponds, VIC 3216, Australia, and also with the Data61, CSIRO, Docklands, Melbourne, Australia (e-mail: {cdnguyen, pubudu.pathirana}@deakin.edu.au).

Jun Zhao is with the School of Computer Science and Engineering, Nanyang Technological University, 50 Nanyang Avenue, 639798 Singapore (e-mail: junzhao@ntu.edu.sg).

Won-Joo Hwang is with the Department of Biomedical Convergence Engineering, Pusan National University, Yangsan 50612, Korea (e-mail: wjhwang@pusan.ac.kr).

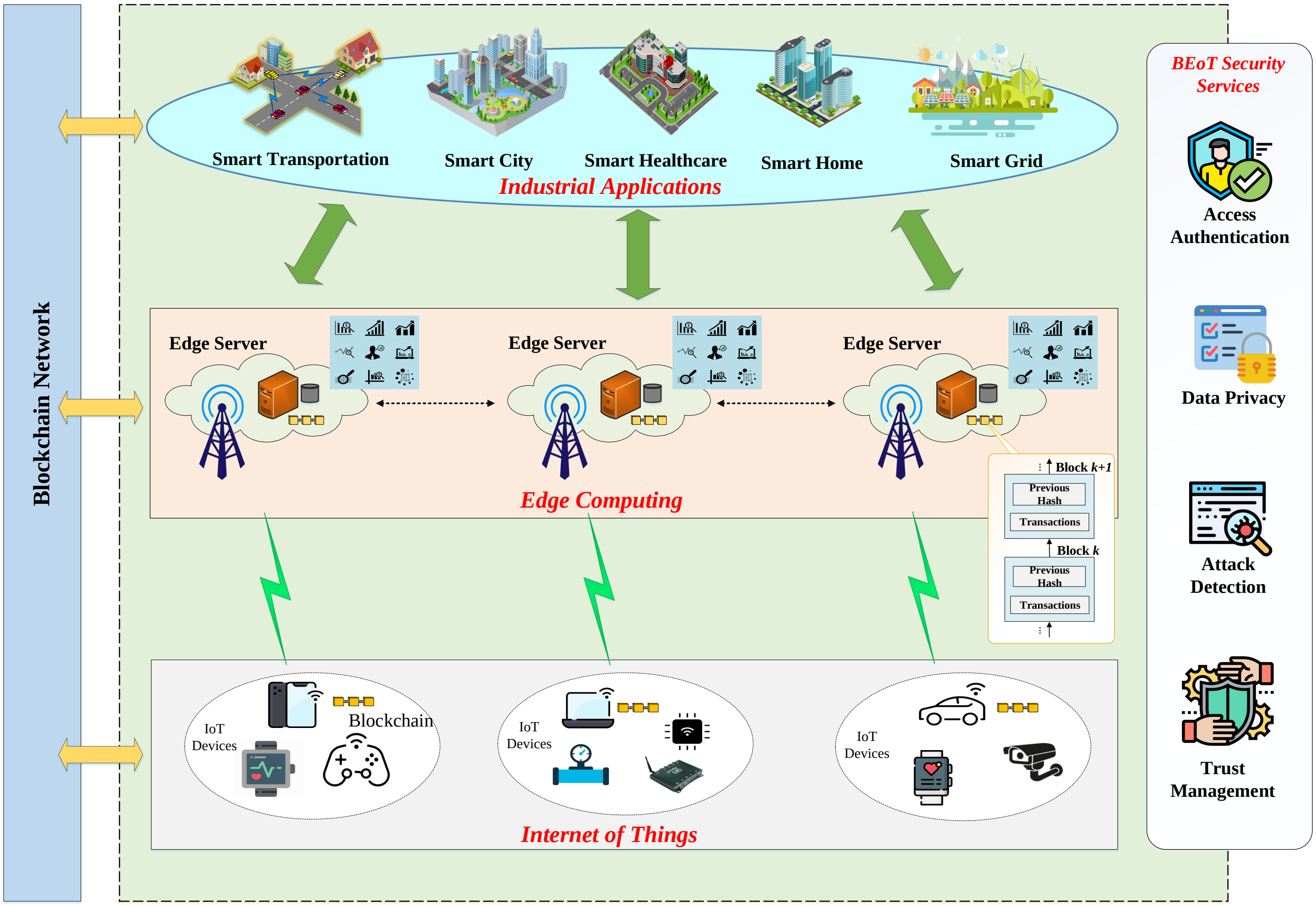

Fig. 1: The generic architecture of BEoT.

- *IoT:* IoT devices such as sensors and mobile phones are responsible for generating or gathering data from the physical environments and then transmit to the nearby edge servers (ES) via access points or base stations. IoT devices with certain resources (e.g. smart phones, laptops) can act as a mobile blockchain entity to make transactions in order to communicate directly with the ES or even join the blockchain mining for extra profits [18]. Other lightweight IoT devices such as sensors can participate in the blockchain network via their representative gateways (e.g., mobile phones) or other mobile blockchain entities in its IoT network [19].
- *Edge computing:* In order to reduce the transmission time, it is necessary for computation nodes to perform data processing near to the end user. Due to heavy network traffic, cost of power consumption increases. To solve these issues, edge computing came into existence. It performs data storage and computing tasks in their edge network within short distance to the end user [7]. As the edge computing nodes are closer to the users, the traffic flow is also reduced. It also minimizes the bandwidth demands and latency in data storage and computation in IoT network. In BEoT networks, IoT devices can offload their data to the ES located at the base stations for processing. ESs are typically equipped with rich computing and storage resources to handle IoT data tasks and provide data services for end users, ranging from data analytics, data prediction to data mining and data storage [20], [21]. Moreover, each ES can also work as a blockchain miner that aims to verify the transactions and produce data blocks for maintaining the blockchain network.
- *Blockchain:* A blockchain is created to form the BEoT system running on top of the EoT network, aiming to interconnect IoT devices, ES and end users together in a decentralized fashion. Particularly, blockchain can guarantee the reliable operations of BEoT systems without the need of a central authority or third-party, by using some key services such as data consensus, smart contracts, and shared ledgers [22].
- *Industrial applications:* BEoT enable new industrial applications, thanks to the application of blockchain in EoT. For example, in a BEoT-based smart transportation system, the secure data analytic services at the edge vehicular servers (i.e., roadside units) under the management of blockchain can support fast traffic control and reliable vehicle routing tasks even in the untrusted vehicular environments [23]. In the following sections, we provide a comprehensive discussion on the use of BEoT in various industrial applications, from smart transportation, smart

city, smart healthcare to smart home and smart grid.

- *Security services:* Enabled by the inherent security properties such as decentralization, immutability, and traceability, blockchains provide a number of important security services for BEoT, including access authentication, data privacy, attack detection, and trust management. The analysis of such security services will be presented in detail in later sections.

B. State of the Arts and Our Contributions

In the literature, many studies on blockchain and EoT topics have been investigated. The works in [24]–[26] present extensive surveys on the use of blockchain and IoT from the different perspectives, spanning across various technical concepts, architectures to research challenges. The potential of blockchain networks in enabling IoT applications and services has also been investigated in [27]. Moreover, the possibility of combining blockchain and edge computing has been investigated and surveyed in [28], [29]. The survey in [30] briefly discusses the role of blockchain in edge computing architectures.

Despite so many research efforts, we have found that a comprehensive review of the use of blockchain in EoT is still missing. Moreover, reviewing the state-of-the-art in the field, BEoT has increasingly attracted much interest, both in academics and industry with a growing number of applied domains and use cases. Motivated by these, we provide an extensive survey on the applications of blockchain in EoT, ranging from applications, opportunities to research challenges and future directions in this article. The key objective of this article is to provide the readers with the state-of-the-art on blockchain and EoT and the recent advances in the BEoT technology. The key contributions of this survey are highlighted as follows.

1) We provide a survey on the state of the art of the applications of blockchain in EoT networks, starting with an updated discussion on the recent developments of blockchain and EoT and highlighting the motivations of the use of blockchain in EoT. Moreover, a high-level BEoT architecture is also proposed and analysed.
2) The key part of this article is focused on the opportunities of BEoT in industrial applications. In this regard, we present an in-depth survey on the use of BEoT in various important application domains, including smart transportation, smart city, smart healthcare, smart home, and smart grid.
3) Furthermore, the security requirements of the BEoT paradigm are also investigated. In particular, we analyze the benefits of blockchain in providing key security services for EoT, such as access authentication, data privacy preservation, attack detection, and trust management.
4) Based on the extensive survey on the BEoT, we identify the potential research challenges and highlight some important future directions in BEoT.

C. Structure of The Survey

The remainder of the article is organized as follows. Section II describes the state-of-the-art in blockchain and EoT. The motivations of the use of blockchain in EoT are also highlighted. In Section III, we survey and analyze the recent development of BEoT technology in a wide range of industrial applications, including smart transportation, smart city, smart healthcare, smart home, and smart grid. The security opportunities due to BEoT paradigm are also presented and discussed in Section IV with some key services, such as access authentication, data privacy preservation, attack detection, and trust management. Section V provides some research challenges and outlines some possible future directions in the BEoT. Finally, Section VI provides the concluding remarks on the core assertions of the paper. A list of key acronyms used throughout the paper is presented in Table I.

TABLE I: ACRONYMS

5G	5th Generation
ACL	Access Control Lists
AI	Artificial Intelligence
DDoS	Distributed Denial-of-Service
DLT	Distributed Ledger Technology
DRL	Deep Reinforcement Learning
EDM	Event-Driven Messages
EDoS	Economic Denial of Sustainability
EHR	Electronic Health Records
EoT	Edge of Things
ES	Edge Server
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineering
IETF	Internet Engineering Task Force
IIoT	Industrial IoT
IoT	Internet of Things
ISO	International Organization for Standardization
ITU	International Telecommunication Union
MEC	Multi-access Edge Computing
PoS	Proof of Stake
PoW	Proof of Work
SDN	Software Defined Network
SGN	Smart Grid Network
SHM	Structural Health Monitoring
SSS	Secret Sharing Scheme
SV	Smart Vehicles
UAV	Unmanned Aerial Vehicle
V2G	Vehicle to Grid
VANET	Vehicular ad-hoc network
VEC	Vehicular Edge Computing

II. Blockchain and EoT: State of the Art

This section presents the background and recent developments of blockchain, EoT, and highlights the motivations of the use of blockchain in EoT.

A. Blockchain

Since the inception of Bitcoin, there is a huge buzz about blockchain. A blockchain is a chain of blocks, which is decentralized and distributed that can store information about transactions [31]. Each block on the blockchain is linked to its immediately-previous block through a hash label. Specifically, a block in a blockchain can store the following information: (i) transaction details like time, date and value of transaction (ii) information about the person who is participating in the transactions and (iii) a unique hash code that differentiates a block from another block. For every transaction, a new block is created and added to the end of the blockchain. The blockchain

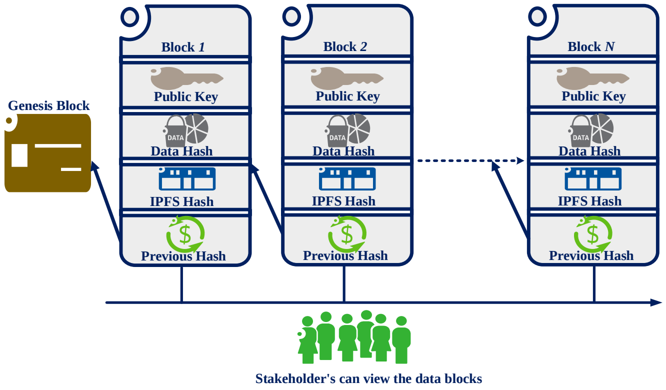

Fig. 2: Blockchain Architecture.

is transparent as all the transactions in the blockchain are stored in a public blockchain and hence can be viewed by anyone. To maintain the privacy of the users, instead of storing their actual names or other information, the encrypted data will be stored in the public blockchain [32], [33]. The block in the blockchain contains the hash of the information in it and also the hash of the block before it. Hence, blockchain is often referred as a decentralized distributed ledger technology [34], [35]. The general architecture of a blockchain is depicted in Fig. 2. If a hacker intends to edit the transaction in a blockchain, he has to modify hash of not only that block but also every other hash following it which is nearly impossible. This security property of blockchain makes it an ideal choice for usage in many sectors like banking, insurance, government services, supply chain management, etc. [36].

Unlike traditional systems which require a central authority to verify and validate the transactions, the transactions in a blockchain are verified and validated by “consensus protocol”. A consensus algorithm is a mechanism where all the participating nodes in the blockchain network agree to the current state of the blockchain [37]. Whenever a new block is created (by transactions) it requires a consensus algorithm to be executed so that all the nodes in the blockchain reach the consensus on the current state of the blockchain. The consensus algorithm is also executed when a new node is added to the blockchain. In this way, consensus algorithms ensure the reliability of the blockchain and also confirm each node in the blockchain as trustworthy [38]. Some of the popular consensus algorithms used today are Proof of Work (PoW), Practical Byzantine Fault Tolerance, Proof of Stake, Proof of Burn, Proof of Capacity [39], [40].

To ensure that the transactions meet the predefined terms and conditions, smart contracts are executed on a blockchain. A smart contract is a program that spans a few lines of code, that are used to make sure that all the transactions follow some kind of pre-agreements. Smart contracts ensure that the transactions are trustworthy. Smart contracts reduce the time which is otherwise spent on verifying the transactions. Accurate decisions can be made quickly because of verification of terms and conditions' verification is automated [41]. The main reasons behind the popularity of blockchain are its unique properties, including decentralization, immutability and transparency.

- **Decentralization**: Before blockchain came into limelight, a centralized entity used to store all the data and all the interactions with the data is through this centralized storage. The centralized systems have several pitfalls like a single point of failure, vulnerability to attacks, etc. These drawbacks in centralized systems can be overcome by decentralized systems as every node in decentralized system stores the information.
- **Immutability**: Due to consensus algorithms, the information stored in the blockchain network is immutable. This property of blockchain makes it an ideal solution for usage in several sectors like finance, supply chain management sectors, governance, etc. [42].
- **Transparency**: The technology used in the blockchain is always open-source. Even the transactions in the blockchain are transparent. The technology or the transactions are secured even though they are transparent as long as the majority of the blockchain network's nodes have to approve the modifications. User information is hidden with the help of complex cryptography algorithms [43].

Even though there are many benefits, there are several key problems with the application of blockchain in distributed systems like IoT. A critical issue is the extensive energy consumption and high network latency caused by running consensus processes such as PoW in the blockchain. This may hinder the applications of blockchain in distributed EoT networks with resource-constrained IoT devices. Another problem is the limited throughput of blockchain systems. For example, Bitcoin can only process a maximum of four transactions/second, and the throughput of Ethereum achieved is about 20 transactions/second, while Visa can process up to 1667 transactions/second [44]. Moreover, security and privacy are other concerns to be considered when applying blockchain to EoT networks. For instance, a serious security bottleneck such as 51% attack can prevent new transactions from gaining confirmations and halt payments between service providers and EoT users. Attackers can exploit this vulnerability to deploy attacks, such as transaction modifications, data breach, adversarial mining operations, all of which can degrade the performance of blockchain networks and results in data privacy leakage issues. Some solutions have been proposed to provide insights on solving these issues. The work in [45] provides lightweight consensus mechanisms to enhance the blockchain performance by compressing consensus storage and designing lightweight block validation schemes, aiming to simplify the blockchain mining process to achieve energy savings and latency improvement. Another study in [46] introduces a mining pool system called SmartPool to improve transaction verification in blockchain mining to protect data privacy and mitigate security bottlenecks, such as 51% vulnerability, ensuring that the ledger cannot be hacked by increasingly sophisticated attackers.

B. Edge of Things

With the improvement in communication technologies and affordable hardware, there has been a rapid growth of smart devices in many areas of daily life and business activities in the past two decades. As information and communication technology (ICT) became affordable, there is an enormous surge in the data generated by mobile phones, IoT devices, industries. The volume of data generated resulted in the use of cloud for storage and computational purposes [47]. Storage and data processing in the cloud have their own challenges like latency, throughput, security, etc. For instance, storage and data processing in real time applications like traffic monitoring in the cloud may not be feasible due to increased latency [47]. The solution to this problem lies in edge computing, i.e., offloading the cloud-computing capabilities to the network edge [47]–[49].

EoT is the integration of edge computing with IoT networks. In EoT, the data acquired by several sensors is temporarily stored in the edge node for real time analytics and predictions [50]. The general architecture of EoT is depicted in Fig. 3. Typically, the data generated from sensors in several IoT applications like smart homes/buildings, smart grids, smart healthcare, smart transportation, industrial IoT, etc. is stored in edge nodes at regular time intervals. Once the data is processed in the edge nodes it will be dissipated to the cloud. Apart from improved latency, EoT offers several other benefits like reduction of traffic to the cloud, improved reliability by installation of applications in close proximity to the edge devices, etc.

C. *Motivations of the use of Blockchain in EoT*

Even though multi-access edge computing is a promising solution for improved services of mobile providers, the security of the data in the edge nodes is a concern [51]. Several applications like connected vehicles, social media apps, healthcare related applications generate the data which is very sensitive [52]. The privacy, confidentiality and integrity of these data have to be strictly maintained. The hackers can even attack the Multi-access edge computing (MEC) with several attacks like distributed denial-of-service (DDoS) attacks, hijacking of cloud servers, ripple attacks, byzantine attacks, injection attacks, etc. to steal the sensitive data from the edge or deny services to the users [53]. Several smart city-based applications such as smart homes, smart grids that generate sensitive data use edge nodes for real time analytics, with a fast throughput. Several industry 4.0 applications also use MEC for analytics in real time [54]. Several applications based on user location like Google Maps, artificial intelligence (AI) based Virtual Assistants use MEC for less latency and predictions/recommendations through machine learning (ML) based algorithms. All the applications mentioned above generate sensitive data of the users such as personal data, health, location, utility services, etc. may possess an elevated risk of compromised security. The properties of blockchain such as distributed nature, traceability, immutability make it an ideal solution to overcome the potential aforementioned problems by applications based on MEC. Blockchain has the ability to prevent issues like identity theft, DDoS attacks, tampering of transactions, user privacy leakages. The use of blockchain in EoT has the potential to be the next revolution in ICT where the mobile application providers can provide safe, transparent, immutable, decentralized applications to the customers with reduced latency, and real-time analytics/recommendations.

The main motivations behind the use of blockchain in EoT are summarized as follows:

- The distributed architectures of EoT will provide a better roof for storing and verifying blockchain transactions.
- By using blockchain, data privacy and security can be well preserved in blockchain-enabled EoT applications.
- The immutability and traceability features of blockchain can be leveraged to ensure the reliability of the transactions in industrial applications such as smart grid, smart transportation, smart health care, government services etc.
- The consensus mechanism of the blockchain guarantees the trustworthiness and transparency of information transferred over the BEoT network.
- The application of blockchain in EoT ensures low-latency response which is increasingly vital for most of the industrial applications.

III. Industrial Applications from BEoT Paradigm

This section presents the industrial applications of the BEoT paradigm highlighting some key benefits. Blockchain with EoT helps to modernize the large computer networks by providing smart architecture to various application domains such as smart transportation, smart grid, smart city, smart healthcare and smart home. These benefits attained through BEoT in aforementioned industrial applications are depicted in Fig. 4.

A. *Smart Transportation*

The term *smart* refers to the idea which helps to build an environment connected with sensors and other computing facilities for better understanding and controlling the user environment. Smart vehicles (SV) have garnered significant attention in recent times due to the advancement of ICT. Smart transportation system enables SVs to get connected to the Internet to access the required data and communicate with each other. The aim of smart transportation system is to provide convenience and comfort to passengers and drivers. It also helps to improve the traffic efficiently and ensures road safety. Vehicles are connected to various network interfaces like WiMax, Bluetooth, and WiFi to communicate with road side units and other vehicles in smart transportation system [55], [56].

Smart transportation systems play a major role in the development of smart cities to keep track of traffic data and to avoid congestion, pollution, accidents etc. Due to the increase in the traffic data, the conventional centralized approach has faced many non-trivial challenges like storage of data, server failure, security, intelligent management etc. If the central server fails, the entire traffic system will be collapsed. Hence a decentralized solution is highly needed. The work in [57] solved the problem by proposing a network model and a blockchain architecture. In this model, the blockchain is integrated with vehicular networking application to provide security and distributed storage for large amounts of data.

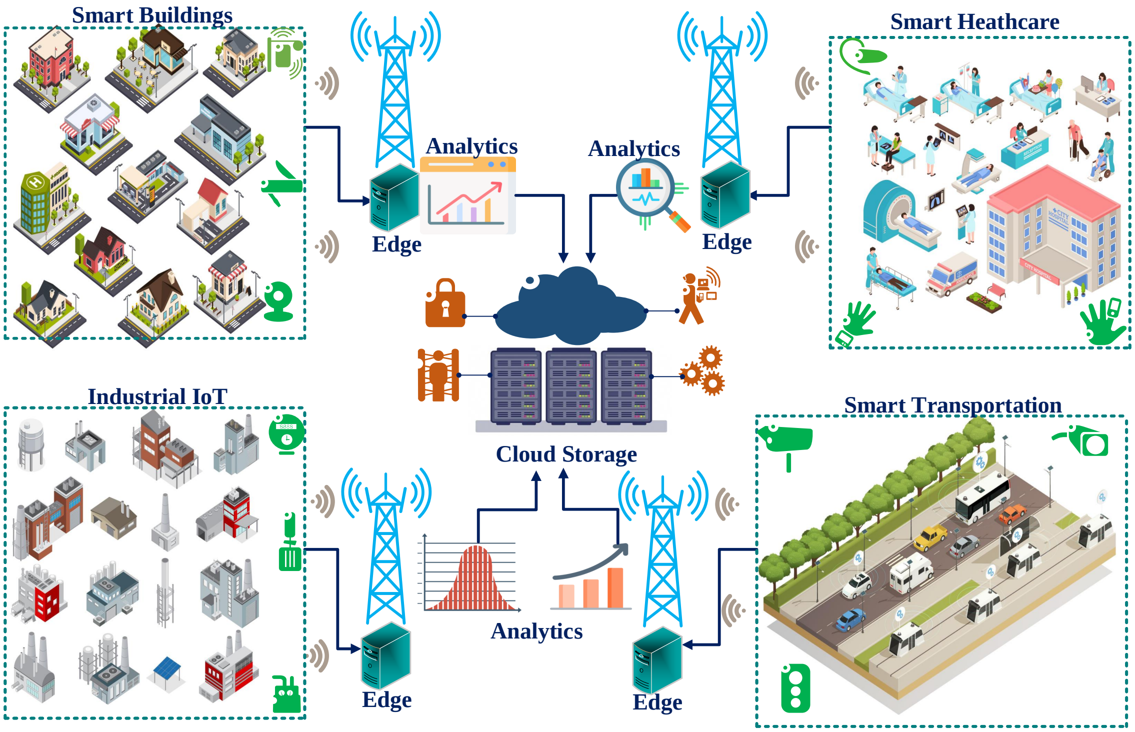

Fig. 3: Architecture of EoT.

Several edge nodes are defined in the vehicle networks such as roadside vehicle and they form sub-blockchain networks. Data blocks in IoV are classified to form several blockchain networks in IoV system.

A platoon driving model was proposed for autonomous vehicles in an urban heavy traffic scenario to avoid congestion, accidents, and pollution. This model groups the vehicles by matching the path successfully in a platoon. Blockchain is integrated in this model in which smart contract is applied for payment purposes which helps in overcoming false and malicious payment transactions. The results proved that the platoon model performed well for individual vehicle models with respect to fuel consumption [58]. Parked vehicle assisted fog computing chain (PVFC) was introduced to accomplish decentralization using blockchain with smart contracts. Also, smart contract design was investigated to monitor the requester and performer behavior with high end privacy and security [59].

Smart transportation applications such as self driving cars produce large amounts of data of different types. To ensure safe driving, sharing of data is required to provide quality service while travelling. Due to lack of resources, vehicular network cannot provide huge data storage and data sharing. A distributed and secure vehicular blockchain was presented by exploiting blockchain consortium for the management of secure data in vehicular edge computing and networks [60].

A multi-agent, autonomous, and intelligent management system was presented in [61] for the safety of the vehicles passing through an intersection point. The system constructed using BEoT enables the communication between vehicle-to-infrastructure and infrastructure-to-vehicle. The system interacts with the vehicles in EoT environment and blockchain ensures the safety of pedestrians and drivers passing through the intersection point. The system helps to reduce the waiting and crossing time of the vehicles and ensures security and reliability. Blockchain supports reliability with decentralization and security by protecting the decisions taken from malicious attacks. EoT helps in increasing the network performance, thereby reducing the latency .

B. Smart Grid

Electricity is one of the greatest inventions, without which today's digital advancements are impossible. Also, the electricity usage increases steadily causing the production to increase. Traditional electrical grids use a centralized structure with millions of components such as power stations, substations, transmission lines and the distribution lines. It cannot accommodate new resource (increasing the load) as it may incur additional overhead leading to power quality issues, i.e. new plants have to be deployed whenever the load is increased. Also, the conventional grid doesn't have a proper prediction system on power blackout, slower response time, insufficient storage and not efficient use of resources. Smart grid overlays the way for smart utilization of the electricity with fewer power outages and lower computational overheads [62]–[64]. The smart grid comprises of smart meters assisted with mobile apps for real-time monitoring of power consumption, electric vehicles (EV), on-demand pricing capability, microgrid, storage, decision support systems, and other smart devices. Smart power grids with its decentralized, distributed framework can strengthen the electrical power of a country through the effective utilization of renewable power resources and contemporary communication advancements. Consequently, this

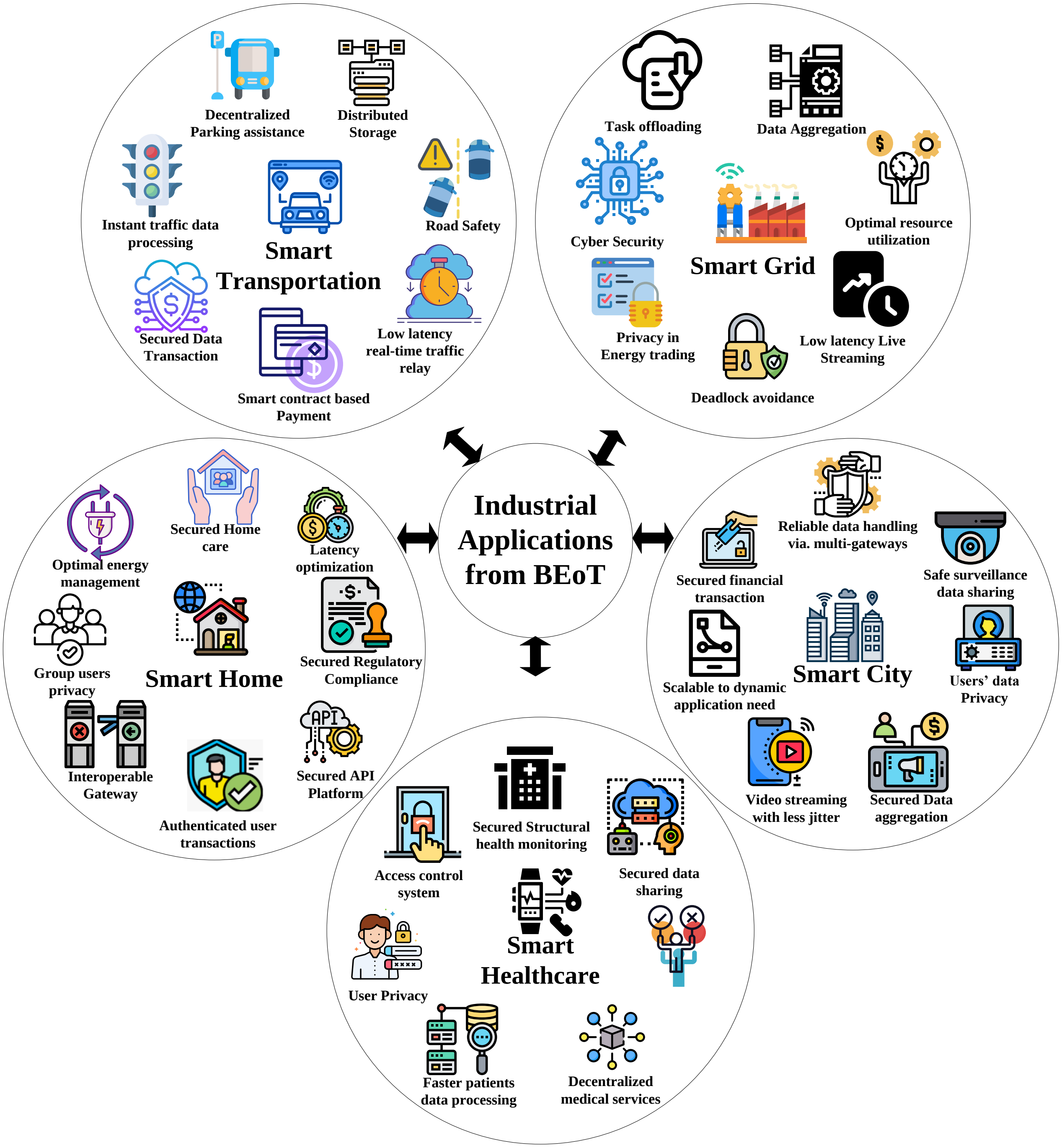
Decentralized Parking assistance
Distributed Storage
Instant traffic data processing
Road Safety
Smart Transportation
Secured Data Transaction
Low latency real-time traffic relay
Smart contract based Payment
Task offloading
Data Aggregation
Cyber Security
Optimal resource utilization
Smart Grid
Privacy in Energy trading
Low latency Live Streaming
Deadlock avoidance
Industrial Applications from BEoT
Optimal energy management
Secured Home care
Latency optimization
Group users privacy
Smart Home
Secured Regulatory Compliance
Interoperable Gateway
Secured API Platform
Authenticated user transactions
Reliable data handling via. multi-gateways
Secured financial transaction
Safe surveillance data sharing
Scalable to dynamic application need
Smart City
Users' data Privacy
Video streaming with less jitter
Secured Data aggregation
Access control system
Secured Structural health monitoring
Secured data sharing
User Privacy
Smart Healthcare
Faster patients data processing
Decentralized medical services

Fig. 4: Industrial applications of BEoT paradigm.

will reduce the power outages and ensures faster restoration of electricity after blackouts.

Smart grid establishes two-way communication between the producer and consumer thereby focusing on making all the consumers as prosumers (they can simultaneously produce and consume electricity). Though smart grid is providing effective services, it has various challenges to be addressed. Some of them are protecting power grids from malicious attacks (integrated security), interoperability in connecting heterogeneous power systems, predicting the stability of smart grids, restoration, determining changing demand patterns, on-demand pricing, lack of regulatory policies, fault detection, and energy management [65], [66]. To ensure secured transactions and to reduce the overheads involved in data processing, blockchain and edge computing can be integrated with smart power grids.

Security concerns of the smart grid network (SGN) include energy security and data security. EVs offer energy management solutions in SGNs through effective energy storage mechanisms. EVs are integrated with the power system and store the power from the grid and load it back to the grid whenever required. The energy trading (charging and loading the EVs) in the SDN-enabled vehicle-to-grid (V2G) infrastructure is a challenging issue. V2G technology of the smart grid reduces the level of demand-supply disparity by strengthening the energy trading capability of EVs. The SURVIVOR-Energy trading in SDN enabled V2G network using blockchain and edge computing framework presented in [67], attempts to cover the tradeoffs in V2G environment. The energy trading decisions are taken at edge nodes closer to the EV to reduce the effects of the processing time, thereby reducing the latency and blockchain is employed to provide security in energy trading transactions. Though the results proved that blockchain is lightweight in terms of communicational and computation cost, content caching, and vehicle mobility remains to be addressed. Similar to [67], a secure framework for energy trading between EV and grid (V2G) in cyber-physical systems was implemented in [68]. Blockchain is used to secure the transactions in energy trading, followed by a contract theory based-incentive mechanism for V2G energy trading. The moderate cost consortium blockchain framework ensures secure V2G energy trading. An incentive contract theory based mechanism attains optimal resource utilization at LEPG. Edge computing is utilized for task offloading with reduced latency and in turn, increases success rate probability in block creation, thereby reducing the computational overhead at local energy aggregators and assists in successful block creation. Results show that there is a 124.6% increase in the successful probability of block-creation.

The convergence of blockchain, edge computing, cryptographic algorithm, and other techniques in the smart grid should not degrade the performance of the SGN. In [69], a lightweight blockchain consortium was presented to ensure the scalability and efficiency of the SGN. Blockchain smart contract is used for managing the key materials table (public key identities) anonymously without exploiting the sensitive information. The security requirements for a smart grid with edge computing are detailed with Proof of Concept, and the model can combat known attacks such as replay attack, stolen verifier attack, and impersonation attack. The model proposed for key management ensures the efficient key update with less computational and communication overhead in comparison to similar models. Henceforth, blockchain with data aggregation can be utilized in SGN for privacy-preserving transactions. Edge computing can be recommended for faster processing or task offloading, thereby providing a low-latency response. Also, to reduce the computational and communication cost with blockchain, a lightweight blockchain framework is recommended. Various industrial applications of blockchains integrated with EoT framework are shown in Table III. It is evident from the literature that BEoT addresses the crucial requirements of the smart systems. Some of them are security, low-latency response, optimized resource utilization, reliability, scalability, and interoperability. Of the various industrial applications, conferred smart city is the one that encompasses the services of other smart systems. For instance, the smart grid supplies the energy required for the operation of other intelligent systems as smart grid utilizes the services of smart transportation for energy trading through EVs. Smart transportation offers various reliable transport services to smart home (safe and comfort life) as well as smart healthcare (instant health services). Blockchain is used for handling all the transactions among the heterogeneous devices in the smart systems ensuring the interoperability and security. ES provides low-latency response in data processing by bypassing the frequent access to the cloud server for all data processing. Thus, the BEoT paradigm paves more significant support in various industrial applications by ensuring interoperable, secured and privacy-preserving data processing.

C. Smart City

As the global population is increasing, it is challenging to meet diverse requirements of service provisions from different users. One of the innovative applications of IoT is the development of smart cities worldwide. Smart cities have the ability to control, monitor, track large volumes of data collected from various sensors installed in the city and provide essential services [70].

Smart surveillance system integrated with IoT technology is one of the vital component of smart city. Some of the smart surveillance applications are face detection, motion detection, license plate detection, and threat detection. A smart surveillance system for smart city was proposed in [71] using microservice architecture and blockchain. The conventional surveillance system is based on monolithic architecture which performs operations such as recording and monitoring whereas it lacks scalability and mostly relies on centralized architectures, which potentially raises security bottlenecks. The proposed microservice architecture decentralizes the operations from various distributed edge devices and proposed scalable solutions to smart surveillance systems.

An architecture was proposed with blockchain to support spatio-temporal smart contract solutions for sharing economy parameters in smart cities integrated with IoT environment. In this architecture, two entities can execute any number of secure transactions using cognitive systems without the need of third party while sharing economy related services using IoT framework for data processing. Cognitive system thinks like human beings and consists of ML algorithms for pattern recognition, natural language processing and data analytics. The cognitive engine is a part of blockchain technology which reads the available data resources from edge nodes and acquire knowledge for reliable decision making. In economy sharing services, transactions are automatic and managed by intelligent cognitive engine without the human intervention [72]. A homogeneous ecosystem was proposed, namely SmartME, in which several applications can be expanded to multinational range by enhancing a shared open ICT framework built for processing, sensing, storage of resources in the network. Several technologies such as cloud, fog, IoT, edge computing, blockchain, ML are required to control the smart city ecosystem [73]. A secure, scalable, distributed network architecture was presented to enhance the strength of evolving blockchain and software defined network (SDN) technologies in smart cities. The architecture includes the features of distributed and centralized network architectures. Edge nodes serve as central server for specific infrastructure and records the credentials and access rules. The edge network helps to reduce the bandwidth of the network and obtain minimum latency. Argon2, a key derivative function based on PoW method was introduced in the proposed architecture in order to improve the security, privacy and abstain leaking information to attackers in distributed smart city network [74].

A framework based on blockchain was presented in [75] for IoT data sharing and privacy preserving in smart city applications. In this work, the blockchain network is divided into various channels and each channel processes the different type of data obtained from various edge nodes such as finance, smart car, smart energy, smart healthcare, etc. Each channel consists of number of certified organizations. Access control within the channel is managed by smart contracts. Security of data in each channel is achieved using encryption algorithms. Thus, BEoT has provided numerous solutions for the decentralization, security and interoperability problems in smart city based applications. Another study was conducted in [76] by combining blockchain with IoT in structural health monitoring (SHM) systems, aiming to improve the operational safety for underground environments in smart cities. In this blockchain based IoT network, the centralized and decentralized distributions are provided by splitting the network into core and edge networks. These networks provide autonomous monitoring and control which improves the scalability and efficiency of the system. Also blockchain based decentralized networks can be deployed to provide efficient and transparent information sharing, security and decision making using smart contracts in SHM.

A BEoT use case on secured SHM in smart city is presented in Fig. 5. The damages in the building are detected based on several factors. These factors are determined by data acquired from an instrumented array of heterogeneous IoT devices such as fibre optic sensors, temperature sensor, inclinometer (tiltmeter and slope detector), accelerometer, strain gauge, vibration sensor, acoustic sensor, smoke detector, transducer, and linear differential transformer. The data is assimilated in the cloud server can be retrieved using the cognitive edge nodes. Cognitive edge nodes are intelligent enough to perform the mining of the data accumulated and early prediction of any problems in the structural health of the building. Smart contracts are used for making decisions, analysis of the type of problems and sharing the damage index of the miner among the edge nodes. For each transaction, a block is added in the distributed ledger assuring authorized access to data and the access privileges to the user. In turn, the notification on the structural health of the building (decisions made through smart contracts) is communicated to various applications and monitoring centres.

Another BEoT use case on safe surveillance data sharing is presented in Fig. 6. Most of the decisions in the smart city environment rely on the surveillance data. Any data transaction, involving these surveillance systems, should be done in a very secured manner. There are diversified video surveillance systems exists in the smart city environment such as video enabled telephone, private video surveillance, commercial building video surveillance, residential surveillance, observation surveillance, road traffic surveillance and health gadget surveillance. Real-time information from many these surveillance systems is required for taking many important decisions. For instance, road surveillance video helps to determine the traffic signal. In turn, crowd gathering information obtained from the commercial building video surveillance determines the reason for the traffic. Also, the acute health issues can be evaluated through health gadget surveillance and more. Videos from these diversified surveillance systems are processed, analyzed and predicted by the video hubs on the edge nodes where blockchain-based smart contracts are deployed for secured and trusted authentication. Furthermore, to avoid overheads incurred in processing enormous data stored at blocks in the blockchain, side chains can be used to segregate unwanted information being stored in the blocks. This will enhance the efficiency of the overall system.

D. Smart Healthcare

Healthcare sector has succeeded in being one of the leading domains with respect to employment and income generation [77], [78]. Even though IoT is contributing to various domains such as smart home, smart agriculture and smart city, its impact on healthcare sector is remarkable. With the development of technologies like IoT, AI, 5th Generation (5G) network, mobile Internet, big data and cloud computing, traditional medical systems are transformed into smart healthcare systems. Using these advanced technologies, smart healthcare systems reduce the threat and cost of medical practices and enhances the progress of telemedicine. Smart healthcare is a medical service that applies technologies such as IoT, AI, wearable devices and mobile Internet to acquire information, link people, tools and organizations associated to healthcare, actively monitors and responds to medical assistance engaging intelligent system. Patients can monitor their health status by using wearable devices, get the medical services through virtual online support systems and the doctors can predict the diseases. Various problems such as security, privacy, transparency, interoperability, decentralization, data storage, and sharing must be addressed for the deployment of smart healthcare systems. Blockchain provides better solution to address these issues in smart healthcare and various research initiatives have been started by integrating blockchain with edge computing [79].

A secure healthcare scheme namely *BHealth* based on blockchain was presented using unmanned aerial vehicle (UAV) in IoT. The UAV collects medical data from the users and stores in nearest MEC server. Basic user information is securely stored in a blockchain using smart contracts. Blockchain synchronizes the health data, secures the data with encryption, verifies the users and allows the UAV to store the data in the server [80], [81].

Blockchain based secure therapy management framework was presented in [82] using MEC for with disabilities in various age groups. The framework was developed by leveraging IoT nodes, blockchain and MEC. Blockchain with MEC provides decentralization, security, low-latency response and data sharing facilities for therapeutic data. The patient is allowed to share their data related to therapy with anyone. The mobile edge network processes the therapy data and

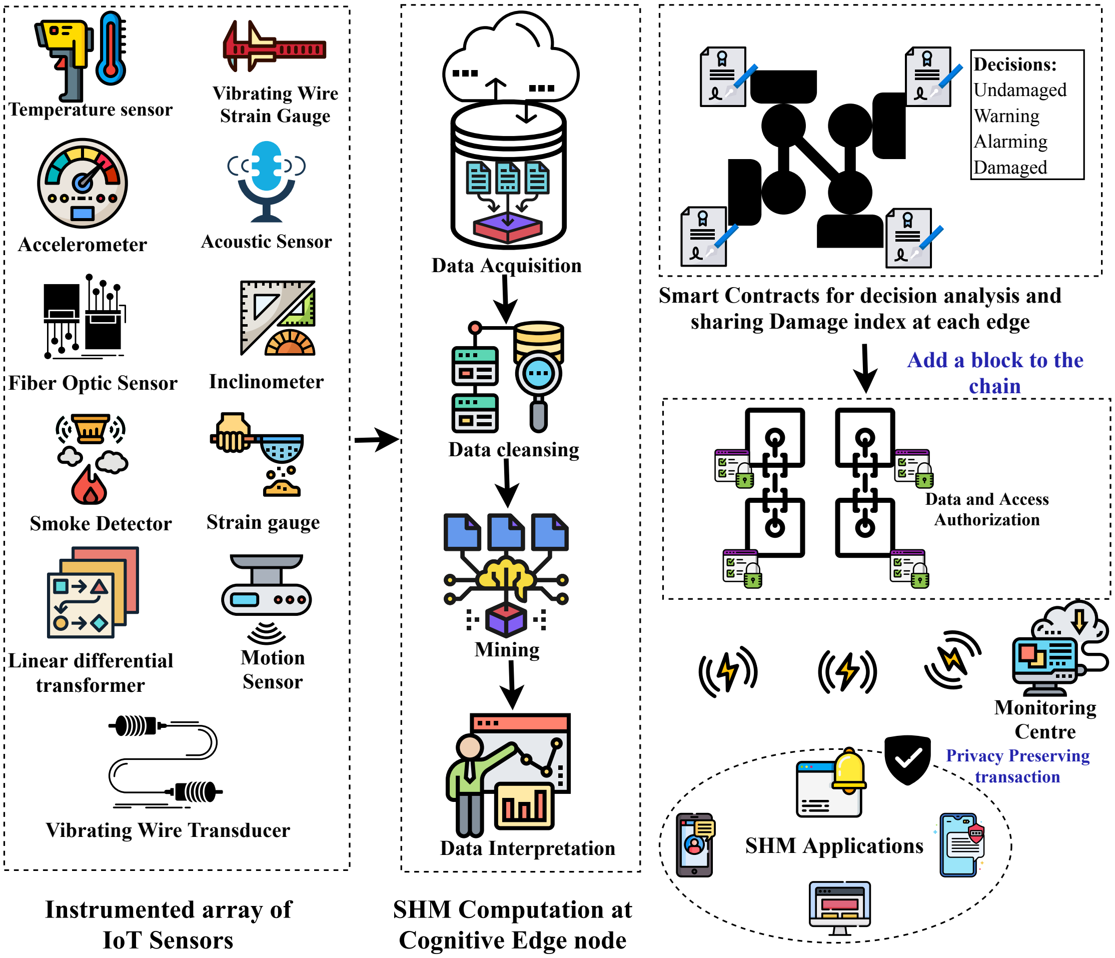
Temperature sensor
Vibrating Wire Strain Gauge
Accelerometer
Acoustic Sensor
Fiber Optic Sensor
Inclinometer
Smoke Detector
Strain gauge
Linear differential transformer
Motion Sensor
Vibrating Wire Transducer
Instrumented array of IoT Sensors
Data Acquisition
Data cleansing
Mining
Data Interpretation
SHM Computation at Cognitive Edge node
Decisions:
Undamaged
Warning
Alarming
Damaged
Smart Contracts for decision analysis and sharing Damage index at each edge
Add a block to the chain
Data and Access Authorization
Monitoring Centre
Privacy Preserving transaction
SHM Applications

Fig. 5: BEoT for secured structural health monitoring in smart city.

prevents the limitations caused by high bandwidth. The related multimedia data such as audio, video and images are stored in a centralized or distributed storage based on the application.

Providing security and privacy to the patient data collected from various sources such as sensors, wearable devices etc., stored in electronic health records (EHR) database is another pivotal challenge in smart healthcare systems. A hybrid architecture using blockchain and edge computing was proposed to provide access control for the EHR data [83]. All the access events are verified and stored using a mutual agreement mechanism before they are included to the blockchain. The EHR data is stored in edge nodes, which apply access control policies to provide attribute based access in association with blockchain. The access control list is executed by the healthcare providers to obtain one time self destructing *URLs* which contain the address of the EHR data. Then EHR data is accessed by the providers using the URLs. Hence, only authorized users who have access to attribute based access control provided by edge nodes can access the EHR data.

A spatial and secure blockchain based mass screening framework was presented for data storage, sharing and management of dyslexia data. The framework analyzes the data and predicts the symptoms of dyslexia. A mobile based multimedia IoT environment was presented to capture the user interaction of dyslexia testing data from a smartphone and share it in the mobile edge network. The edge node applies auto grading algorithms on the data for predicting dyslexia symptoms and the final results are stored in the blockchain. Blockchain provides decentralized data repository for captured multimedia based IoT test data shared for medical research and analysis [84].

E. Smart Home

In this world of digital computation, people are committed towards their work, so it is harder for an individual to be constantly vigilant on household chores. Smart home, with ICT assisted devices make the home a safer and better place to live. One of the critical use cases of a smart city is a smart home. The smart home uses the Internet, to interconnect all the household appliances for facilitating seamless communication between the residents and the home appliances. Some of the remotely controlled functions in a smart home are closed circuit television, air conditioners, television, lighting systems, speaker, thermostat, temperature, refrigerator, doors, and pet feed. Any appliance with the capability of the remote access can join the smart home network and can be controlled through a laptop, PC, a smartphone or a tablet. This interconnection

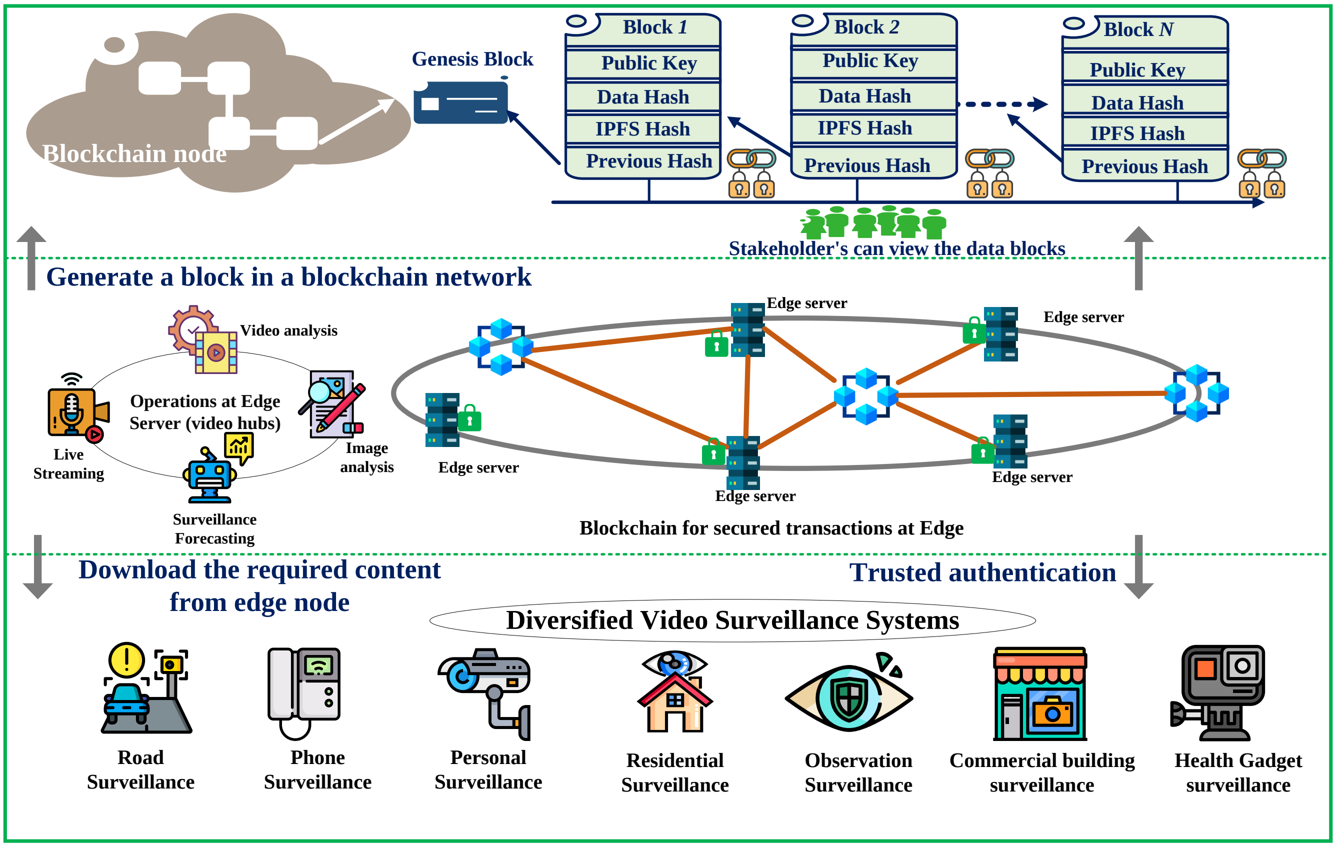

Fig. 6: BEoT for safe surveillance data sharing in smart city.

of objects is possible through IoT devices which makes use of the Internet to connect all the objects with the ability to share electronic information. The general types of alerts raised by these smart household devices are motion detection in case of theft, automatic control of home appliances upon its unwanted usage, healthcare of home ridden older people, kids activity monitoring, etc. The alert system will send alert notification not only to the home residents but also to the concerned security providers in case of theft, the fire station in case of fire, blue cross services in case of animal ill-treatment and ambulance service for health care issues. Therefore the primary concern for implementation of smart home system is security and privacy. Also, this concern paves the way for a lot of security threats in terms of data theft and cyber-attack, such as DDoS exploiting all the network bandwidth for hijacking the environment. Furthermore, application of blockchain in the smart home helps to protect all the IoT devices in smart homes and data acquired from these devices for establishing interconnection among heterogenous applications while participating as an IoT node in the smart city blockchain network.

Data access from the Internet-enabled smart home appliances will be easier for the adept hackers, the users of technology. So, the work in [85] presented a blockchain-based gateway architecture to prevent data theft by malicious users. Multiple security interventions in centralized gateway architecture of the smart homes are addressed, and severe network attacks are counterfeited. The data transaction among various devices in the smart home network are carried out only for the devices registered in the gateway. The blockchain is incorporated in this gateway layer of a smart home network which records and authenticates the devices joining the network through a SHA2 encryption algorithm, thus avoiding the data theft. The additional computational complexity incurred by blockchain at the gateway can be reduced by adopting edge computing for offloading the computation overhead. The proposed BEoT framework prevents the gateway from the attacks, namely blockchain 51% attack, patch file forgery attack and DDoS attack.

A secure authentication system integrating blockchain (for ensuring reliability in user transactions), group signatures (GS) (to authenticate different devices in the network) and message authentication code (for authenticating gateways) was implemented in [86]. This model not only provides a solution for critical challenges in blockchain applications, but it can also efficiently trace the footprints of the intruder misbehaviour.

Remote monitoring of patients in a smart home using a fog assisted IoT based in-house patient monitoring system was presented in [87]. To avoid the unprecedented delay caused by processing the data to and from the cloud, the three-layered model proposes the fog computing services with notification mechanisms at the network edge (i.e., in the gateway). The proposed model offers real-time interactive services on event classification with minimum latency at the fog layer. Fog assisted IoT model can effectively monitor various behaviors of the patients and provides real-time notification on the behavior of the patients with minimum delay in processing.

TABLE II: Unique requirements of blockchain in industrial applications.

S.No	Industrial applications	Common problem	Unique requirements of blockchain	Challenges in blockchain adoption
1	Smart Transportation	Stabilized network, uninterrupted and secured data sharing among edge devices and other public vehicles	Blockchain can be utilized for uninterrupted and secured data sharing and privacy to retain the efficiency of ITS	Vulnerable to cybersecurity attacks during real-time data sharing and optimized resource utilization
2	Smart Grid	Secured energy trading among prosumers	Blockchain for secured and privacy-preserving energy trading transaction in edge computing-based smart grids	Resource optimization (communicational and computaional resources)
3	Smart City	Secure data sharing by users for facilitating varied smart applications (multiple trust domains)	Blockchain for secured and transparent data-sharing among users and multiple trust domains	Scalability issues when the number of transactions increased
4	Smart Healthcare	Distributed authorization of edge nodes, security and data privacy in healthcare data records	Blockchain ensures data privacy in more sensitive health care data transactions and restricted third party data access	Security issues pertaining to key management; Scalability issues when the number of transactions increases and lack of standardization
5	Smart home	Access control issues to different residents and visitors	Blockchain can be used for users privacy requirements and enabling secure data sharing among non-interoperable that party service providers	Vulnerable to security attacks while intact with the consensus process and scalability issues when the number of applications increase

The model performs the accurate classification of events based on the behavior of the patients in the smart home using BBN with temporal mining.

Furthermore, a ChainSDI (Software Defined Infrastructure) framework implemented in [88] influences blockchain along with edge computing to provide a secure sharing and computation of smart home patients data. The framework attempts to address the data interoperability and regulatory issues in emerging SDIs used for healthcare applications. ChainSDI is an API on SDI that serves as a testbed for any healthcare application. Though ChainSDI provides better security and privacy in handling users transactions, the communication and computation cost is increased.

The industrial applications discussed in this section used edge computing enabled services for low latency response. Also, these industrial applications interact with each and exchange their services. The edge enabled smart environment faces significant challenges in security and privacy space such as authentication, access control, intrusion detection as the ES are heterogeneous and migration of services across these servers are prone to various security threats. Blockchain with EoT can address these issues, and the unique requirements of blockchain in these smart applications are depicted in Table II.

IV. Security Requirements from BEoT Paradigm

This section presents the necessary requirements of BEoT paradigms through some of the key benefits of EoT protection. Today, modern businesses use a vast, growing systems of wireless devices and data-intensive applications [89]. As more devices are added and computing power moves closer to the device, traditional networks will not be able to maintain the level of performance required by the businesses [90]. The nature of the work accomplished by IoT devices creates a need for much faster connections between the data center and the devices [91]. Edge computing moves computational power relatively close to the users, applications and devices where data is generated and the actions are needed to be taken. Approaching the data source closer can bring positive real business impacts such as better user experience, improved performance, data security, uninterrupted operation [92]. In today's increasingly digital world, cybersecurity is a top concern for business, government and individuals. As millions of devices connect, hackers find new vulnerabilities to deliver increasingly sophisticated attacks, making it much harder for systems to identify, protect and respond to these threats [93]. In addition to stealing intelligence or disrupting business activity, hackers now have more entry points allowing them to damage our physical world and pose serious security risks to utilities, factories, transportation and other critical infrastructure. Blockchain technology is one of the solutions to meet these security requirements in EoT through transparent transactions. The blockchain ledger catalogues each transaction series from end to end, enabling the reliability, synchronisation and tracking of all transactions. [94].

A. Access Authentication for Edge of Things

Smart IoT technologies are designed to make our lives simpler. Various cellular networks offer seamless connectivity for billions of things or devices. To protect the exchange of data, device manufacturers need to provide unique and reliable digital identities and ensure secure data exchange [95]. Blockchain provides security against hacking, enables end-to-end encryption of the data they share [96].

Some previous studies employed blockchain technology to protect EoT applications like smart grids, smart transport, smart medical devices, smart cities, etc. Some researchers focused on efficient authentication and data sharing between different platforms [97]. The work in [98] introduces a method for improving distributed, trusted authentication services on blockchains and the EoT. Byzantine error tolerance consensus algorithm was proposed to develop a blockchain for data storage and authentication. Edge computing was applied to a blockchain by providing two edge nodes, a resolution edge node, and a cache node. Resolution edge nodes provide name resolution, and the caching node aims to provide edge authentication using smart contracts and helps to improve the hit ratio. The asymmetric cryptography model was proposed to address security challenges between terminals and nodes. The experimental results show the algorithm's efficiency in terms of effective communication and computing costs, while

TABLE III: Survey of industrial applications of BEoT paradigm.

Applications	Ref.	Contribution	Technologies used	Key features
Smart transportation	[58]	Platoon driving model for urban IoVs	Blockchain, IoV, edge cloud	A vehicle platooning mechanism assists to obtain path information matching, smart contract based payment mechanism in urban road traffic condition
	[59]	Parked Vehicle assisted fog computing chain	Blockchain, smart contract, fog computing	Provides decentralization and security for parked vehicle assistance in vehicular network using blockchain with smart contracts
	[60]	Vehicular blockchain	Blockchain and edge computing	Utilizes vehicular blockchain and smart contracts to obtain data storage, sharing and security in vehicular network
	[61]	Multi-agent road safety system	Blockchain, EoT	Ensures safety and security using blockchain, and enhances network performance and latency reduction using EoT
Smart grid	[67]	Energy trading in SDN enabled V2G network	SDN,Blockchain,Edge computing and EVs	SDN enabled EVs offer less latency and Lightweight-blockchain with reduced computational overhead provides security in processing the energy transaction.
	[68]	Secure V2G energy trading	Blockchain, Edge and contract theory	Blockchain ensures secure V2G energy trading, contract theory optimal resource utilization and EC ensures task offloading with low latency
	[69]	Mutual authentication system in SGN	Blockchain and edge computing	Almost all the security requirements of the edge enabled SGN was met with lower computation and communication costs for key management
Smart city	[72]	Sharing economy services in smart city	BIoT, cognitive edge nodes assisted with AI	Financial transactions are automatic and managed by intelligent cognitive engine in Blockchain without the involvement of human using edge computing
	[73]	SmartME	Fog, BEoT and ML	SmartME scales up the applications to wide range by enhancing open sharable ICT and applies edge, fog, blockchain to control the smart city ecosystem
	[74]	Hybrid network architectural framework	BEoT and SDN	Offers the features of both distributed and centralized architectures. Edge node serve as central server and records the credentials thereby reducing the latency
	[75]	Secure framework for IoT data sharing	Blockchain, IoT, edge computing	The framework divides the network into multiple channels and each channel secures the data related to specific application collected from edge devices
Smart healthcare	[80]	BHealth	Blockchain, smart contract and MEC	The scheme synchronizes the health data, secures the data with encryption, verifies the users and allows the UAV to store the data in the ES
	[82]	Therapy management framework	BIoT and MEC	The framework for the differently abled people provide decentralized, secured, low-latency response and therapeutic data sharing facilities
	[84]	Blockchain based mass screening framework	BEoT in mobile and auto-grading algorithms	Provides decentralized data repository for captured multimedia based IoT test data shared for medical research and analysis.
Smart home	[88]	ChainSDI, regulatory compliance	SDI, Edge Computing and Blockchain	Provides secured specification for regulatory compliant requirement in data processing and a low-latency response in health care-related data processing

the proposed model outperforms existing models by reducing the delay rate of 6%-12% and increasing the hit rate 8%-14%. However, the proposed model can be enhanced by reducing latency while transferring large data packets to the destination.

In a real-time environment, achieving minimal latency with high security is a challenging task. In [69], the authors proposed an authenticated blockchain model with an effective key agreement protocol for the smart grid edge-computing systems. Experimental results promise security improvements with minimal latency for smart grid growth. The proposed model focused more on providing better security, although the computing cost can be minimized by maintaining the ES cache nodes. In a similar wok in [99], the authors proposed a secure key agreement protocol using blockchain for smart grid edge computing systems. The main requirement of this proposed model is that the smart meter sometimes fails to check the authenticity of the electrical power control, and therefore, the authentication process is not achieved at a better rate. Transferring goods safely from source to destination using supply chains requires high bandwidth, which can be achieved with 5G enabled EoT. In [100], the authors proposed blockchain-based authentication technology integrated with the RFID supply chain system in 5G enabled EoT for efficient computing and communication costs. The proposed authenticated model works on cryptographic hash and bitwise XOR rotation. Initially, the authors considered N blocks, and each block has the privilege of a reader tag. The reader tag must prove its identity by transferring the authentication message to the supply chain. The supply chain validates the received message and ensures acknowledgment. Experimental results achieve a higher security rate with effective communication costs compared to existing models. In addition, the proposed model can be extended further to focus on a real-time problem.

The rapid growth of vehicular edge computing (VEC) in smart transport has intensified the implementations on traffic systems. Accessibility of communication channels, authentication of privacy and trust management in automobiles have made VEC highly prevalent. In [101], the authors proposed a VEC blockchain model based on trackable map directions using dynamic route hash chain. This model's vision is to build a decentralized, secure system with low communication overhead. Moreover, the proposed model does not achieve better latency and communication overhead for a 256-bit data message, thus inhibiting its usefulness in VEC. Another interesting work to provide authentication in electric vehicles integrated with cloud infrastructure and edge computing [102], the authors proposed blockchain-based data coins and energy coins on a decentralized network. During this process, blockchain technology enhances authenticated data processing and security mechanisms for energy transmission. However, the proposed model does not specify how data manipulation, identification are carried out, thus limiting its use in the VEC. Another application of blockchain for efficient data sharing in VEC can be found in [103], where the data can't be shared without proper authorization. The vehicular blockchain model uses smart contracts to accomplish effective and reliable information storage on roadside units (RSUs) and information sharing within automobiles. The reputation-based access control technique is used to make sure the transmission of reliable information between vehicles. The experimental results for the detection of abnormal vehicles at a trust threshold of 0.35 is 100% for the proposed model, while the other existing model is only 50%.

B. Data Privacy for Edge of Things

Data privacy is one of the key requirements that protect data from malicious access. A number of data privacy mechanisms available include encryption, decryption, perturbation-based, and blockchain. Data is securely transmitted in the blockchain by maintaining timestamps and hash functions. Shared information is distributed across multiple sites using a distributed ledger [104], [105]. In [106], researchers propose a privacy-preserving method by assigning tasks to the edge nodes using smart contracts, in which each block keeps the assigned task information. All edge nodes connected to a decentralized network and the information is distributed using alias function in the blockchain. Edge nodes need to perform the assigned task and calculate time and energy consumption. Experimentation performed on a variety of privacy methods to prevent the storage of block information from multiple data mining threats. Moreover, the proposed model achieved a satisfactory privacy rate; however, it can be improved by focusing more on optimizing energy consumption at edge nodes. The successful development of the smart grid depends on the transformation of secure communication technologies, as the smart grid offers multiple options for collecting electrical data [107]. However, smart grid applications face challenges like energy security and privacy protection. In [108], the authors proposed preserving BEoT 's privacy for smart grid applications. In this process, electricity consumption can easily be traced without disclosing end-user information to identify inappropriate energy-using behaviors by raising alarms using blockchain. Few supernodes are deployed in the blockchain responsible for resource allocations that validate the edge nodes. Here edge nodes are considered smart meters, power sensors. These edge nodes distribute the energy to the end-user, which reduces the burden on the central system and helps to improve the computing process. The edge node is validated using the covert channel authorization scheme, and the access control scheme. Validation is designed to ensure that a 51% attack ensures that the majority of participants are good. Optimal allocation of energy resources will be made through a smart contract, covering three elements, including energy consumption, latency, and security of communication. The work in [109], introduces a distributed IIoT model for smart factory using blockchain. In order to ensure proper privacy, the authors introduced the bell-la padula (BLP) approach, which is integrated with the biba model [110]. Experimental findings show that the proposed model provides enhanced security and privacy features. However, the proposed model failed to achieve proper resource allocation strategies, thereby reducing its usefulness. In [111], the authors proposed an innovative blockchain model for edge-based IoT architectures called LiTichain with multiple blocks, each with a finite lifespan. The block will be removed from the chain if the life of the transaction expires. LiTichain is created by merging two different graphs. One graph represents the life of the transaction, and the second graph represents the formation of a block in the chain. As the number of transactions increases the height of the chain, the authors have introduced a K-height block method to restrict the height of the chain. The experimental results are obtained by taking New York taxi IoT data, which transmits sensed data to the ES. The ES will collect and process the data. The proposed blockchain model is used on ES to ensure sensed IoT data privacy.

C. Attack Detection for Edge of Things

Due to the proliferation in IoT sensing technology, attackers can attack and steal sensitive and vital data. Some applications, such as smart grids, smart cities, supply chains, healthcare, etc., are often used to generate sensitive IoT data and there is a high probability of attacking these data. Cyber attackers are exploring different vulnerabilities to exploit highly sophisticated attacks, making it extremely difficult for systems to identify, protect, and respond to such attacks. The attack detection system is one of the requirement to monitor the communication system and to protect against malicious attacks [112]. Recently, the authors in [113] introduced a new blockchain architecture by integrating edge, cloud and SDN to achieve confidentiality and strengthen the security mechanism by preventing IoT devices from various types of malicious attacks. During this process, IoT sensors from different locations capture the data and transfer the captured data to the edge-cloud for pre-processing. The SDN-enabled blockchain process allows dynamic network traffic management and detects malicious attacks. In the cloud layer, most attacks are identified and eliminated, which reduces storage space and increases the rate of latency while reaching the edge layer; therefore, the rate of attack is drastically reduced, increasing the performance in terms of throughput and delay. Experimental results obtained by deploying 100 nodes in the 3000 m × 3000 m search area, taking into account energy consumption, packet delivery ratio, throughput and delay as performance metrices. The results promise that the proposed security model will consume less energy and improve the transfer of packets with better throughput and delay. In addition, the proposed model does not produce any results for the detection of attacks, thus limiting its utility in the blockchain model. Another blockchain framework can be observed in [114], where the economic denial of sustainability (EDoS) are prevented from malicious attackers. Secret sharing scheme (SSS) is introduced to provide security whenever the ES fails. Sometimes, whenever the ES is down due to some malicious attack by an attacker, the proposed model uses a binary search mechanism to identify and locate the afflicted ES. The results reveal that the proposed model uses 128-bit ciphertext data, 256-bit Diffie-Hellman key, requires 0.004 ms for encryption, and 0.0039 ms for decryption. The total computational time taken by the proposed model for uploading and accessing data is 14.1199 ms. In addition to computational performance, the proposed model achieves a better attack prevention rate. Event-driven messages (EDMs) in vehicle networks will be generated during the occurrence of accidents, road slipping. EDMs consists of photos, videos, etc. and faces several challenges, such as security and latency, during the transmission of these messages. The work in [115] introduces a reliable blockchain platform with 5G-enabled vehicle edge computing to transfer EDMs to end-users by optimizing communication costs. During this process, EDMs are transferred to nearby ES in order to reduce the response time. Blockchain technology is used at the edge nodes to track messages and protect messages from a variety of attacks. The results show that the proposed model protects EDMs from different types of attacks, like impersonation attacks, DDoS attacks, Masquerade attacks, and reduces communication overheads. Another interesting work related to VEC [116], the authors integrated deep reinforcement learning (DRL) and blockchain into vehicle networks aim of providing smart and reliable caching content. During this process, initially the proposed blockchain model ensures a decentralized data caching system in which the vehicles perform data caching and maintains an authorized blockchain at the nearby fixed base stations. Later DRL is used to develop an optimal data caching model by considering mobility as one of the metrics. Finally, to enhance the process of block verification, the authors used the new Block Verifier Selection Method, proof-of-utility (PoU).

D. Trust Management for Edge of Things

Due to the rapid growth of technical advances, large amounts of data are gathered from edge nodes or IoT devices, but data protection, trust management and privacy are very important requirements on ES, particularly when the collected data is malicious and can cause serious problems. The work in [117] introduces a blockchain-based, trusted data management system (BlockTDM) in edge computing. In this process, the blockchain model is designed to ensure mutual authentication, smart contract and flexible consensus. The proposed BlockTDM ensures the privacy of data through the provision of a multi-channel data segment. The data is encrypted using user-defined encryption techniques just before the transaction is stored in the blockchain. Decryption and transaction of data in a secure blockchain is carried out using hyperledger as a smart contract. Another exciting blockchain application can be found in [118], which preserves MEC from fake service record threats and malicious edge threats. The authors proposed an RL algorithm to decrease computational latency, optimize energy consumption, and reduce the resource allocation time of the edge devices. The experimental results show that the authors used the blockchain model on Ethereum, PoW protocol is used to promtly build service records in the blockchain. The proposed model reduces the malicious attack rate by 66.4%, optimizes energy consumption by 10.5%, and reduces latency by 67.4%. In [119], the authors introduced a decentralized, trustworthy blockchain model in edge computing. The domain name server sends the user request to the appropriate ES, which reduces the propagation delay. To achieve trustworthiness and security, all participants involved in transactions must share their block information and transaction details. Participants contributing to the network will earn blockchain tokens. The experimental results show that the proposed model provides 12.54% optimal latency rate compared to the other existing model. Another interesting work in [120] suggests a trust-aware IoT data economic system (TIDES) to provide safe, precise, and intelligent IoT data trading systems for the end-users. In the first step, the trustworthiness mechanism obviates malicious distributors to ensure secure transmission of data. In the second phase, the game-theory based pricing method facilitates win-win transactions where suppliers get better quality information at a reasonable rate and distributors get huge returns. In the third phase, if the candidate has accidentally made a transaction to a malicious distributor, the payment of the transaction will be reflected automatically. In the final phase, TIDES uses an MEC model to reduce latency and overhead storage. The experimental results show that TIDES accomplishes better results in terms of trading time, reduced latency, better security and communication costs.

E. Summary

In this section, we examined the security requirements of the BEoT paradigm and benefits of blockchain in providing essential security services to EoT, such as access authentication, data privacy, attack detection, and trust management. In today's world of advancements in Internet, wireless technology, and data-intensive applications, we have seen significant technological changes in data communication and networking applications. Edge computing is a trending technology designed to improve latency and increase computational performance. As millions of devices connect, hackers find new vulnerabilities to exploit sensitive and confidential data. Blockchain technology can remove all these security problems through transparent transactions. We summarize security opportunities from the BEoT Paradigm in Table IV.

V. Research Challenges and Future Directions

This section presents the key research challenges and future directions related to the BEoT paradigm.

A. Research Challenges

BEoT has the potential to spot its avenues in almost all kinds of digital applications. BEoT paradigm is an integration of three giant technologies, namely blockchain, Edge computing, and IoT. It offers significant benefits combating many issues in the performance of deploying each other separately. Therefore the issues concerned with these technologies should be addressed.Some of the challenges of the BEoT paradigm are discussed here.

1) Security in blockchain: Blockchain is a shared, secured, immutable, decentralized, and valid ledger, which records and tracks the transactions done on digital resources without the necessity of centralized authority in various domains such as smart healthcare and smart cities. It enables two users to exchange and communicate in a peer-to-peer network where the distributed decisions are taken by considering the majority vote instead of a single centralized administration. Blockchain has demonstrated its ability in many applications which involves a centralized ledger. Some of the promising applications of blockchain are monitoring the network and providing security services which includes privacy, confidentiality, and integrity. Despite several potential applications of blockchain in various domains, it still has many open-ended challenges. The various security, privacy, and scalability challenges of blockchain are cryptokey management, data privacy in chain management,

TABLE IV: Review of security requirements of the BEoT paradigm.

Security services	**Ref.**	**Application Domain**	**Contributions**	**Challenges**
Access authentication	[98]	IoT system	Edge nodes provide name resolution, and the caching node provides edge authentication using smart contracts	Poor latency and delay while transferring large data packets
	[69]	smart grid	1. The key agreement protocol ensures secure communication between the end user and the ES 2. Smart contract ensures secure transaction, identity verification, recording of the public key	Results limited to authentication did not show computation cost results
	[99]	smart grid	The key agreement protocol enables smart meters to acquire reliable power services from distribution control through a single private key	Smart meter sometimes fails to check the authenticity of the electrical power control
	[100]	service system	Cryptographic hash and bitwise XOR rotation are used for authentication.The reader tag must prove its identity by transferring the authentication message to the supply chain	Proposed method not investigated on a real-time issue
	[101]	vehicular network	Trackable map directions using dynamic route hash chain and to build a decentralized, secure system with low communication overhead	The model does not achieve better latency and communication overhead for a 256-bit message
	[102]	vehicular network	Authenticated data processing and security mechanisms for energy transmission	Proposed model does not specify how data manipulation, identification are carried out
	[103]	vehicular network	Smart contracts are used to accomplish effective and reliable information storage on roadside units	Resource allocation at edge nodes is excluded
Data privacy	[106]	IoT network	Edge nodes connected to a decentralized network and the info is distributed using alias function in the blockchain	Proposed model can optimize the energy consumption at edge nodes
	[108]	smart grid	Few supernodes are deployed in the blockchain responsible for resource allocations that validate the edge nodes	The model does not specify traffic load and resource allocation as the network size increases
	[109]	IIoT	BLP approach integrated with the Biba model [110] to ensure data privacy	Proposed model failed to achieve proper resource allocation strategies
	[111]	IoT network	LiTichain blockchain model is created by merging two different graphs. One graph represents the life of the transaction, and the second graph represents the formation of a block in the chain	Poor latency and delay while the number of transactions increases
Attack detection	[113]	IIoT	The SDN-enabled blockchain process allows dynamic network traffic management and detects malicious attacks	Proposed model does not produce any results for the detection of attacks
	[114]	service system	EDoS are prevented from malicious attackers, SSS is to provide security whenever the ES fails	Proposed method not investigated on a real-time issue
	[115]	vehicular network	Reliable blockchain platform with 5G-enabled vehicle edge computing to transfer EDMs to end-users by optimizing communication costs	System design does not focus on anonymity
	[116]	vehicular network	DRL-blockchain aims to provide smart and reliable caching content on vehicle networks	Proposed model uses tiny dataset
Trust management	[117]	IoT network	1. BlockTDM ensures the privacy of data through the provision of a multi-channel data-segment 2. Data encryption is carried out using user-defined encryption techniques and decryption is done by hyperledger as a smart contract	The system design does not reduce communication overhead
	[118]	Mobile computing	1. RL algorithm to decrease computational latency time, optimize energy consumption, and reduce the resource allocation time of the edge devices 2. PoW protocol is used to build service records in the blockchain quickly	The proposed model does not specify resource allocation as the size of the network increases
	[119]	Storage network	1. The domain name server sends the user's request to the ES to reduce the propagation delay 2. To achieve trustworthiness and security, all participants share their block information and transaction details	Results did not show computation cost results
	[120]	IoT network	1. Game-theory based pricing method facilitates win-win transactions 2. TIDES uses MEC model to reduce latency and overhead storage	Not effective for large real-time data

transaction linkage, and compliance with regulations with respect to data privacy. Several research works have been carried out on the privacy of the users in various digital scenarios. Blockchain technology was developed to deploy the Bitcoin cryptocurrency and resolves the double spending issue. The solution for this problem is bitcoin in which all the transactions are made public in the ledger. Any node can track and watch the transactions which are spent. But the problem is the complete anonymity is not guaranteed in bitcoin [121]. In the distributed EoT, ES are distributed at the network edge, making the ES vulnerable to security attacks. The conventional cryptographic techniques are difficult to be accommodated in ES as they are resource-constrained. This challenge in EoT opens up a need for a secured lightweight authentication where the ES can authenticate the end devices at a faster pace. Furthermore, the edge server needs a trust management mechanism to ensure reliable trust computation between end nodes and various ES as these servers cannot carry trust among other servers.

2) Standardization: Blockchain was originated as an infrastructure to provide solutions for the digital cash problem. Also, it allows payment across borders irrespective of the constraints in the geographical area over the Internet. Whereas it takes many days to transfer funds between various banks located in different countries using the conventional banking system. This open nature of blockchain technology makes it further expanded to address many commercial problems in several financial applications, Industrial sectors, IoT, supply chain, etc. But the speed and extent of implementation of blockchain technology are obstructed by its interoperability challenges. These challenges are not only due to the representation of various digital tokens and cryptocurrencies but also the vital differences in the behavior of transaction management. This makes blockchain difficult to combine with other conventional enterprise systems and interoperate. This eventually creates issues for the regulatory acceptance of blockchains, thereby raising a need for standardization.

3) Resource management in BEoT: The decentralized blockchain framework empowers the robustness and scalability of the system by utilizing the optimal resources from all the nodes, thereby reducing the latency in the data processing as well as making the resource-restricted IoT platform a robust resource utilization framework. On the other hand, IoT encompasses the devices with restricted bandwidth, whereas blockchain consumes more bandwidth. BEoT, a distributed platform where the heterogeneous data (distributed in different areas) from heterogeneous nodes are accumulated and processed in a distributed environment. Therefore, the various distributed resources like data centres for storage, robust machines for complex computation, interoperable middleware services, user details can be managed effectively. The distributed ledger at every node in blockchain alleviates the need for a centralized server by storing the device credentials and transactions. As the number of IoT devices is increasing, the number of transactions in the ES also increases rapidly. Therefore higher processing capability and computational network resources are required to ensure the increased processing capability and low latency responses.

The storage overhead incurred due to this massive processing requirement of blockchain in processing real-time data streaming, can be reduced by segregating the metadata required from the original data stream and minimizing the contents to be stored on the blocks. Though lightweight blockchain serves this purpose, its scalability will decrease with an increase in the number of network nodes. Therefore, sidechains can be used with blockchain as a control layer [122]. The major problem in the integration of IoT and blockchain is storage constraint, i.e., a combination of resource-constrained IoT with high resource-consuming blockchains. Resource-constrained edge devices with limited computing resources are not efficient in handling numerous transactions when integrated with huge resource consuming blockchain frameworks. The decentralized blockchain framework trust mechanisms will ensure trustworthiness in data from edge nodes [123].

1) **Scalability:** Scalability is a more significant issue in the data storage of cloud-centric IoT devices. As the blockchain grows with the number of users or transactions, it is difficult for the IoT devices to store the ledgers as it increases in size. Furthermore, IoT devices range from low-power to high-end servers. So, depending on the resource capability of the IoT device, designing a device-specific blockchain is a trending challenge. This includes the security algorithms, efficient mining process, and appropriate metadata segregation from the ledger.
2) **Intelligence:** The BEoT paradigm offers various services like secure and privacy-preserving data sharing with low latency response for various industrial applications. It still lacks intelligence in processing and prediction the future behaviour of the applications. For instance, earlier prediction of disease in smart healthcare based on the information accumulated in the edge, demand response prediction and EVs lifetime prediction in smart grids, traffic data prediction in intelligent transportation systems, resource demand prediction in smart cities and predictive maintenance of home appliances requires intelligent agents to enable predictive analytics in almost all industrial applications of BEoT.

The resource management issues concerned with various applications of Blockchain, IoT, and edge computing individually as well as in combination is presented in Table V. It is evident that resource management directly impacts the acceptability, scalability, robustness, interoperability, load provisioning, long-term sustainability, faster data processing (with low-latency response), and task offloading. Henceforth, to design a scalable and secured BEoT environment hosting of the resources, metadata segregation in blocks, faster (higher bandwidth) and controlled access to the resources must be enforced.

B. Future Directions

This section presents the various solutions and future directions in BEoT with AI and 5G networks.

1) Solutions to Research Challenges: Various research solutions in the literature had addressed the challenges in the BEoT environment.

- **Security Frameworks:** The work in [124] discusses various security problems and services provided by blockchains. One of the advantages of blockchain is its pseudo-user anonymity feature, but there is a threat that the user information can be exposed to hackers. The users are not anonymous, in which blockchain-based access control lists(ACL) associate the ACL with the users directly. The same problem occurs in blockchain-based provenance and key management. The anonymity problem of blockchain is solved by bitcoin in which the public key of the user is their identification. A trust enabled blockchain framework called trustchain for privacy preserving transactions in EoT was proposed in [125]. Trustchain, lightweight permissioned blockchain (consent violation) ensures privacy preservation among its prosumers and avoids unprecedented delays in distributed networks. Furthermore, as the edge computing moves computing resources closer to the end users, the privacy of data should be ensured in distributed computing environments.
- **Standardization bodies:** An initiative for standardization has been started on blockchain through a professional

committee of International Organization for Standardization (ISO), World Wide Web Consortium (W3C) International Telecommunication Union (ITU), Institute of Electrical and Electronics Engineering (IEEE) and Internet Engineering Task Force (IETF). ISO develops standards for nomenclature, terminology, ontology and architecture, privacy, identity, security, interoperability, smart contracts, and Governance. The W3C is a standardization organization produced web standards and they have started a community group for blockchain to develop standards for message format, guidelines for storage in private and public blockchain, torrent, and side chain. The ITU has created a focus group on distributed ledger technology (DLT) to recognize and examine the services and applications of DLT, to create guidelines and practices for the implementation of these services and applications in the global market. IEEE has created a project for blockchain; namely standardization initiative for the blockchain framework in IoT. IETF defines suite for Internet protocol for interoperability standards and network communication for blockchain technologies [126].

- **Scalable Architectures:** Skyline Queries are added benefits in optimal dataset query processing. These queries will help to retrieve the results from an optimal-related set instead of searching the whole dataset. This, in turn, reduces the data processing time and removes the overhead in storing larger datasets [127]. The resource management framework using blockchain proposed in [128] alleviates the tremendous amount of energy consumed by processing the explosive data accumulation at the cloud data centers. Though edge computing offers low latency response, edge nodes have a limited capacity, which makes it difficult when the user demand increases [129]. This leads to constrained access to IoT devices and undetermined network latency. The virtual resources are hosted on the edge nodes with blockchain for managing these transactions [130]. Access control to the devices is provided by blockchain through the management hub [131] on the edge of the sensor networks. Furthermore, these IoT devices are more vulnerable to various security attacks because of their resource constraints. So a permission blockchain with Edge computing, namely EdgeChain, was developed in [132].

2) Other Future Directions and Enabling Technologies: Though multiple issues were solved in literature, the BEoT should be compatible and upgraded itself for known and unknown future problems. Therefore these challenges should be addressed before the full-fledged adoption of BEoT. Some of the future directions in the BEoT environment that evolves as the technology advances are usability, cybersecurity, memory management, Access control for resources and users, real-time data stream delivery, and predictions on future trends and patterns [133].

Enhancing Blockchain Performance for the Betterment of BEoT: Though blockchain is secure, the blockchain security issues discussed in terms of challenges and the vulnerabilities imposed by ES and IoT devices will have a greater impact on the future BEoT framework. Furthermore, the ability of blockchain to store entire transaction data may create storage burden leading to scalability issues. This ability of blockchain consumes more energy, network bandwidth and thereby reducing the throughput. As the IoT devices will be increasing rapidly, the scalability and storage issues will significantly impact the performance. Therefore a lightweight consensus mechanism should be incorporated for blockchain mining processes by segregating the appropriate data from the ledger and storing it in side chains [122]. Also, data inconsistency due to proliferation of nodes in the lightweight blockchain will remain. Although skyline queries provide effective data processing, data privacy still remains a baffling issue [127]. A lightweight blockchain framework with efficient data processing and service validation, alleviating the scalability issue will be a research direction for future BEoT. Bigdata processing systems will be an essential candidate to handle the enormous data accumulations. Also, the bigdata processing will provide effective processing of data in resource constrained ES to ensure low latency response.

Integration of AI and BEoT: As BEoT lacks intelligence required for predictive analysis in smart applications, AI will provide a more sophisticated solution. AI aids the machines to mimic the natural intelligence possessed by humans [134]. These intelligent agents (AI incorporated machine) were programmed to simulate the cognitive behavior of the human and their brain, which is specifically utilized for solving problems in real-time through experience (learning) [135]. AI have bought remarkable automation in many domains utilizing computational schemes. This led to the revolution of smart computing systems. Some of them are robots in military applications (mission-critical activities), health care assisted robot in monitoring patients in the absence of surveillance, automated transportation (anonymous operated autonomous vehicles), gaming applications, content delivery network (routing), marketing (making all predictions on single search), chatbots (online agent, a virtual assistant to handle customers) in finance, agricultural robots, rovers in space research, and social networking (predictive analysis).

The notable subsets of AI are ML and deep learning (DL), the most significant technological advancements. Indeed, there are numerous technical challenges in the BEoT paradigm that can be assisted by the AI's smartness. Privacy preservation is the prominent issue in the mission-critical application of BEoT standard. The study in [136] have suggested the integration of AI at edge nodes aiming at the higher level of the privacy to the users with fewer security vulnerabilities by alleviating the use of third parties to mine the data at the edge. The proposed model suggests the storage of processed data in blocks instead of storing the raw data and retrieving it back for processing later. Edge AI allows the end devices to control all the mining processes through Ethereum smart contracts (where the data owners can update their policies involved in data processing and sharing) directly, which enables to reduce considerable network bandwidth. Furthermore, they indicate that data owners at the edge can process their data using neural network algorithms and make valuable predictions as the immutable nature of blockchain records all the transaction involved in mining.

Labelling of datasets in AI empowers the model. It provides better performance, but the traditional crowdsourcing (generating labels from the human input) is centralized and have various issues such as data privacy and delayed processing. Furthermore, training the DL models from the local edge server requires larger storage and computing power, which is not feasible with resource-constrained edge devices. The training of models can be shifted to the cloud and can be retrieved for the processing, which may lead to data privacy issues. Therefore, Edgence, a framework proposed in [137] provides decentralized crowdsourcing and decentralized AI training with blockchains for secured and privacy-preserving data transactions in decentralized IoT applications. Thus, blockchain ensures the privacy of the data allowing the data owners to negotiate their data usage by third parties and the robust AI algorithms processing at the edge, thereby drastically reducing the network latency and the load on a block in a blockchain transaction. The survey in [138] have explored the broader perspectives of blockchain and edge computing applications. One of the more extensive areas addressed is the contribution of AI in blockchain-based edge computing applications and its benefits. With evidence from the literature, they have suggested that AI will tremendously impact the performance of BEoT, especially in resource management, automatic generation of smart contracts, prediction of faults, and scalable off-chain computation at the network edge.

In-edge AI framework in [139] was proposed for the effective utilization of the interaction among the mobile edge nodes to train the AI models with a reduced computational load. They have employed the DL techniques like DRL to attain optimal caching at edge nodes with minimal computation and federated learning for managing the resources effectively. Furthermore, they suggest that the blockchain framework can be integrated with this environment, but load distribution among heterogeneous edge nodes remains unexplored and will be a research direction.

Cognitive Edge: Cognitive edge is an interesting idea in the edge computing space that utilizes the cognition from AI algorithms for processing at the edge effectively. A blockchain-based optimal knowledge paid sharing for AI-enabled edge nodes was introduced in [140]. For effective knowledge aggregation with reduced computational load, knowledge management chain and knowledge trading subchains are deployed. ML algorithms are used for knowledge extraction. AI-enabled edge nodes are priced for knowledge sharing due to their imposed selfishness. The blockchain consortium based on smart contracts uses knowledge coins for knowledge trading among Edge AI nodes. This ensures tamper-resistant (knowledge coins are stored in knowledge managers), decentralized and very fair trading. The green blockchain Proof-of-Trading combines the PoS and PoW for reduced resource consumption. Thus the optimal pricing will encourage smooth knowledge trading among buyers and sellers in AI edge nodes.

On the other hand, sharing the economy-related services in smart environment, leverages computational load as well as incurs the security burden. Sharing economy related services and smart contracts have a tremendous impact on the massive BEoT crowd. Blockchain and AI-based cognitive edge framework was designed in [72] for facilitating the sharing economy-related service in a smart city. The proposed model uses DL algorithms for extracting the meaningful and significant event information from the IoT data. The framework uses cognitive edge nodes for storing and processing the immutable ledgers of blockchain and off-chain (includes the transactions involving IIoT and mobile edge devices). The model integrates the cognitive processing at the edge for sharing economy-related services. AI is used for data processing and extracting shareable economy-related data from heterogeneous IoT devices, blockchain and social network media.

Furthermore, as the number of IoT devices in the smart environment increases, the traffic generation will increase tremendously leading to higher back-haul data rates. Intelligent caching is performed to overcome this, by storing popular contents at different locations of the network. But still, this has a more significant challenge in decision making based on future content popularity. This can be resolved with DL and reinforcement learning for significant decision making on cache content prediction [54]. Therefore, when AI is integrated with the BEoT environment, it reduces the computational power, increases data processing rate and scalability, increases the decision making in load management and intelligent caching, and predicts any system attacks in advance. The major security concerns and resource optimization with the use of blockchain for EoT can be alleviated with the power of CE. All these can be achieved without human intervention but through the intelligent agents mimicking the human cognition. The greatest challenge in this adoption is to focus on the effective training of the AI models in heterogeneous environments. Because the machine is trained through learning from previous experience, but training or learning in a dynamically changing environment is challenging and can impact the overall performance. One of the most common solutions suggested in the literature is retrieving information from all the heterogeneous nodes for training the model, but its effectiveness is still unexplored and paves a way for future research.

BEoT in 5G: The emerging 5G network is 20 times faster than the current 4G LTE used in almost all cellular networks [141]. It can carry a huge payload in a shorter duration by its variety of spectrum bands. The scalable BEoT environment requires higher computational resources with low latency response. Also, BEoT applications demand peer to peer communication for its transactions, 5G has the more suitable capabilities for hosting the BEoT. Both technologies drive each other forward. As 5G sorts out the communication constraints in blockchain and blockchain ensures the privacy concerns. 5G infrastructure crowdsourcing using smart contracts, 5G infrastructure sharing (i.e., national roaming and spectrum sharing) without a third party, the most challenging international sharing, network slicing to accommodate multiple users with seamless interaction, massive machine communication and low-latency ultra-reliable communications. The massive adoption of 5G with blockchain has particular hindrance such as managing throughput with scalability, transforming an enormous number of contracts in 5G into smart contracts, need for regulatory compliance, privacy, cloud infrastructure costs, and a trusted registration system [141]. Usually, the more powerful 5G cellular network with edge computing is integrated with AI for effective mining of big data accumulated in the edge nodes as ineffective mining may degrade the system performance. And blockchain cryptocurrencies namely, bitcoin and litecoins can be utilized for the privacy-preserving virtual transaction [142]. Also, the major cost incurred in handling the cloud infrastructures can be reduced by using Edge intelligence (edge computing with distributed AI). The edge enabled 5G-blockchain-based infrastructure for scheduling distributed heterogeneous edge resources was proposed in [143].

The intelligent transportation framework in [144] was developed to address the reliable security scheme requirement of the vehicular ad-hoc network (VANET) with enhanced vehicle trust management in traffic monitoring. 5G-VANET with SDN is used to ensure the utmost reliability and global traffic network control. The immutable ledger blockchain with centralized authentication is used to secure the traffic system from malicious vehicles (the vehicle that violates the traffic rules and regulation) by creating hazardous traffic in the network. Blockchain stores the vehicle details, traffic tag details of its travel path and vehicular messages in the blocks. Also, blockchain is utilized to offer trust management by computing the trust value through the integration of PoW and PoS. The simulation results guarantee the better privacy preserved trust management for IoT vehicular networks. The use of blockchain in 5G MEC unlocks the new business value, brings new value shift, and captures this value in the telecommunication industry. The low-latency communications of 5G are attained through edge computing. The privacy concerns in heterogeneous MEC are solved by blockchain. The blockchain is constructed to enhance user privacy as well as privacy of network topologies (attained using accommodative bloom filter without revealing the topology privacy by maintaining the routing consensus) [145]. Their integration is fulcrum behind the excellent results in 5G BEoT supply chain management [100] and unmanned vehicular systems [146].

The summary of challenges, future directions, its application and benefits of BEoT is described in Table V.

VI. Conclusion

In this article, we have conducted an extensive survey of the use of blockchain in EoT networks and associated applications. We have first introduced an overview of the blockchain and EoT and discussed the main motivations behind the use of blockchain in EoT networks. Furthermore, we have also provided a generic BEoT architecture where IoT, edge computing, blockchain and succeeding applications and security services have been analyzed. Subsequently, we have paid attention to the review of the BEoT adoption in a number of important industrial applications, including smart transportation, smart city, smart healthcare, smart home, and smart grid. The security benefits of the BEoT paradigm have been discussed, with some key services such as access authentication, data privacy preservation, attack detection, and trust management. Finally, we have outlined some research challenges and pointed out open research directions toward BEoT-5G networks. We believe that this article will instigate exemplary approaches on BEoT research for future applications and services.

References

[1] "Cisco edge-to-enterprise IoT analytics for electric utilities solution overview," 2020. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/big-data/solution-overview-c22-740248.html

[2] L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[3] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: a comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[4] A. 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*, vol. 17, no. 4, pp. 2347–2376, 2015.

[5] H. El-Sayed, S. Sankar, M. Prasad, D. Puthal, A. Gupta, M. Mohanty, and C.-T. Lin, "Edge of things: the big picture on the integration of edge, IoT and the cloud in a distributed computing environment," *IEEE Access*, vol. 6, pp. 1706–1717, 2017.

[6] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2017.

[7] L. Nkenyereye, J. Y. Hwang, Q.-V. Pham, and J. S. Song, "Virtual IoT service slice functions for multi-access edge computing platform," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11 233–11 248, 2021.

[8] P. P. Ray, D. Dash, and D. De, "Edge computing for Internet of Things: A survey, e-healthcare case study and future direction," *Journal of Network and Computer Applications*, vol. 140, pp. 1–22, 2019.

[9] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the Internet of Things: Security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, 2017.

[10] K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-preserving multi-channel communication in edge-of-things," *Future Generation Computer Systems*, vol. 85, pp. 190–200, 2018.

[11] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *IEEE Access*, vol. 8, pp. 16 440–16 455, 2020.

[12] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22 328–22 370, 2019.

[13] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based e-health systems," *IEEE Access*, vol. 7, pp. 66 792–66 806, 2019.

[14] J. Pan, J. Wang, A. Hester, I. AlQerm, Y. Liu, and Y. Zhao, "Edgechain: An edge-IoT framework and prototype based on blockchain and smart contracts," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4719–4732, 2018.

[15] Y. Ren, F. Zhu, J. Qi, J. Wang, and A. K. Sangaiah, "Identity management and access control based on blockchain under edge computing for the industrial Internet of Things," *Applied Sciences*, vol. 9, no. 10, p. 2058, 2019.

[16] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-VN: A distributed blockchain based vehicular network architecture in smart city." *Journal of Information Processing Systems*, vol. 13, no. 1, pp. 184–195, 2017.

[17] N. Islam, Y. Faheem, I. U. Din, M. Talha, M. Guizani, and M. Khalil, "A blockchain-based fog computing framework for activity recognition as an application to e-healthcare services," *Future Generation Computer Systems*, vol. 100, pp. 569–578, 2019.

[18] K. Suankaewmanee, D. T. Hoang, D. Niyato, S. Sawadsitang, P. Wang, and Z. Han, "Performance analysis and application of mobile blockchain," in *2018 international conference on computing, networking and communications (ICNC) Maui, Hawaii, USA*, 2018, pp. 642–646.

[19] I. Buldin, M. Gorodnichev, S. Makhrov, and E. Denisova, "Next generation industrial blockchain-based wireless sensor networks," in *2018 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF) Sankt-Peterburg, Russian Federation*, 2018, pp. 1–5.

TABLE V: Challenges, Future Directions and Benefits of BEoT.

Ref.	**Challenges**	**Application**	**Description**	**Benefits**
[122]	Massive real-time data streaming and storage overhead in the lightweight blockchain	Smart home and surveillance systems	Segregation of metadata through lightweight blockchain to scale down processing time and edge computing to reduce latency	Acceptability, long-term sustainability and scalability
[127]	Inefficient mining process when the users are increased and skyline query processing in blockchain	Any smart systems	Energy-efficient consensus protocol design for mining the application-specific data to be stored on the ledger	Scalability, robustness and faster data processing
[128]	Massive explosion of data will consume more energy and the cost will be higher	Smart grid system	Decentralized blockchain-based resource management with embedded reinforcement learning for request migration in smart contracts	Cost minimization in energy consumption in power grids
[129]	Load distribution when the networks scale up devices and safety loading	Cloud-centric IoT	Provisioning of virtual resources and permissioned blockchain for access control in edge nodes	Low-latency response and secured transaction
[130]	Edge computing resource allocation	Mobile blockchain	Number of entries in the block must be optimal, an economic model with optimal resource utilization	Optimal resource utilization, low-latency and scalability
Ref.	**Future direction**	**Application**	**Description**	**Benefits**
[131]	Global storage of different resource access control details into the blockchain	IoT devices in smart environment	Decentralized blockchain where the access control policy of the entire system is stored in a single blockchain	Scalability
[132]	On-demand resource provisioning to heterogeneous IoT devices	Smart systems	Permitted blockchain to link IoT devices and the resources on the edge nodes and credit (internal coins)-based resource management	Scalability, secure auditing and data logging
[136]	BEoT mining at edge nodes by alleviating raw content in the block	Edge AI for smart health care	Edge AI is used for local decision making at edge nodes.	Reduced network resource consumption at the edge
[138]	BEoT resource management and reinforced security management policies	AI's neural networks in blockchain	ML and DL algorithms improve the efficacy of BEoT paradigm with reduced energy in distributed computation	Scalable mining at the edge, low computation overhead and vulnerability analysis
[139]	MEC task offloading, resource management and load distribution when integrated with blockchain	AI learning models in blockchain	DRL to attain optimal caching at edge nodes with minimal computation and federated learning for resource management	Cognitive computing, effective task offloading and optimal edge caching
[140]	Knowledge trading for AI-based BEoT environment	Knowledge gaining via. ML and DL	Knowledge chain with sidechains is used for decentralized, tamper-resistant, confidential and fair pricing of AI-enabled edge nodes	Aggregated resource management and fair knowledge pricing
[141]	Transforming an enormous number of contracts in 5G into smart contracts	Blockchain for 5G	System must ensure scalable transactions in handling numerous smart contracts with low cost and secured authentication mechanisms	Scalability and standard regulatory compliance for blockchain
[144]	Trust management in SDN enabled 5G vehicular adhoc network	5G intelligent transportation system	Blockchain assures privacy concerns in 5G with 5G with vehicle privacy and secured traffic monitoring	Trust management and malicious node detection
[143]	Secure edge services under more complex industrial networks	Blockchain with 5G in IIoT	A DRL algorithm is used for edge resource management (cross-domain sharing) in 5G beyond IIoT applications	Cross-domain resource sharing and scheduling, tamper-resistant resource management
[146]	Extracting untapped value in 5G MEC	5G BEoT in supply chains and UAV	Describes how blockchain absorbs the value created by the 5G MEC in the telecommunication value chain	Automated new business value creation permanent, verifiable and transparent transactions
[145]	Privacy protection of MEC	Trust management in diversified MEC	Blockchain for ensuring user privacy and network privacy in multi-server collaboration	Trusted routing in collaborative network and privacy in network topology

[20] S. Garg, A. Singh, K. Kaur, G. S. Aujla, S. Batra, N. Kumar, and M. S. Obaidat, "Edge computing-based security framework for big data analytics in VANETs," *IEEE Network*, vol. 33, no. 2, pp. 72–81, 2019.

[21] S. Yi, Z. Hao, Q. Zhang, Q. Zhang, W. Shi, and Q. Li, "Lavea: Latency-aware video analytics on edge computing platform," in *Proceedings of the Second ACM/IEEE Symposium on Edge Computing*, 2017, pp. 1–13.

[22] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *Journal of Network and Computer Applications*, p. 102693, 2020.

[23] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Network*, vol. 32, no. 3, pp. 78–83, 2018.

[24] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2018.

[25] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32 979–33 001, 2018.

[26] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.

[27] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to IoT applications and beyond," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8114–8154, 2019.

[28] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, 2018.

[29] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making knowledge tradable in edge-AI enabled IoT: A consortium blockchain-based efficient and incentive approach," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6367–6378, 2019.

[30] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

[31] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," National Institute of Standards and Technology, Tech. Rep., 2018.

[32] K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, "Differential privacy-based blockchain for industrial internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4156–4165, 2019.

[33] M. Baza, N. Lasla, M. Mahmoud, G. Srivastava, and M. Abdallah, "B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1214–1229, 2019.

[34] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications*, vol. 126, pp. 45–58, 2019.

[35] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, 2019.

[36] N. Deepa, Q.-V. Pham, D. C. Nguyen, S. Bhattacharya, P. B, T. R. Gadekallu, P. K. R. Maddikunta, F. Fang, P. N. Pathirana *et al.*, "A survey on blockchain for big data: Approaches, opportunities, and future directions," *arXiv preprint arXiv:2009.00858*, 2020.

[37] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2906–2920, 2019.

[38] G. Kumar, R. Saha, M. K. Rai, R. Thomas, and T.-H. Kim, "Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6835–6842, 2019.

[39] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020.

[40] S. Ma, Y. Deng, D. He, J. Zhang, and X. Xie, "An efficient nizk scheme for privacy-preserving transactions over account-model blockchain," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 641–651, 2020.

[41] S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. Guizani, "Securing smart cities through blockchain technology: Architecture, requirements, and challenges," *IEEE Network*, vol. 34, no. 1, pp. 8–14, 2020.

[42] E. Politou, F. Casino, E. Alepis, and C. Patsakis, "Blockchain mutability: Challenges and proposed solutions," *IEEE Transactions on Emerging Topics in Computing*, 2019.

[43] Y. Zhang, C. Xu, J. Ni, H. Li, and X. S. Shen, "Blockchain-assisted public-key encryption with keyword search against keyword guessing attacks for cloud storage," *IEEE Transactions on Cloud Computing*, 2019.

[44] "Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2521–2549, 2020.

[45] L. Luu, Y. Velner, J. Teutsch, and P. Saxena, "Smartpool: Practical decentralized pooled mining," in *26th {USENIX} Security Symposium ({USENIX} Security 17)*, 2017, pp. 1409–1426.

[46] Y. Liu, K. Wang, Y. Lin, and W. Xu, "Lightchain: A lightweight blockchain system for industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3571–3581, 2019.

[47] Q.-V. Pham, F. Fang, V. N. Ha, M. J. Piran, M. Le, L. B. Le, W.-J. Hwang, and Z. Ding, "A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art," *IEEE Access*, vol. 8, pp. 116 974–117 017, Jun. 2020.

[48] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," *Future Generation Computer Systems*, vol. 97, pp. 219–235, 2019.

[49] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Secure data sharing and searching at the edge of cloud-assisted Internet of Things," *IEEE Cloud Computing*, vol. 4, no. 1, pp. 34–42, 2017.

[50] J. Zhao, Q. Li, Y. Gong, and K. Zhang, "Computation offloading and resource allocation for cloud assisted mobile edge computing in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 8, pp. 7944–7956, 2019.

[51] S. Chen, Z. Pang, H. Wen, K. Yu, T. Zhang, and Y. Lu, "Automated labeling and learning for physical layer authentication against clone node and sybil attacks in industrial wireless edge networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 2041–2051, 2020.

[52] M. Alazab, M. Alazab, A. Shalaginov, A. Mesleh, and A. Awajan, "Intelligent mobile malware detection using permission requests and API calls," *Future Generation Computer Systems*, vol. 107, pp. 509–521, 2020.

[53] B. Hussain, Q. Du, B. Sun, and Z. Han, "Deep learning-based DDoS-attack detection for cyber-physical system over 5G network," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 860–870, 2020.

[54] L. U. Khan, I. Yaqoob, N. H. Tran, S. A. Kazmi, T. N. Dang, and C. S. Hong, "Edge-computing-enabled smart cities: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10 200–10 232, 2020.

[55] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2794–2830, 2019.

[56] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K.-Y. Lam, and L. H. Koh, "Blockchain for the internet of vehicles towards intelligent transportation systems: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4157–4185, 2020.

[57] T. Jiang, H. Fang, and H. Wang, "Blockchain-based Internet of vehicles: distributed network architecture and performance analysis," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4640–4649, 2018.

[58] C. Chen, T. Xiao, T. Qiu, N. Lv, and Q. Pei, "Smart-contract-based economical platooning in blockchain-enabled urban Internet of vehicles," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4122–4133, 2019.

[59] X. Huang, D. Ye, R. Yu, and L. Shu, "Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 2, pp. 426–441, 2020.

[60] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660–4670, 2018.

[61] A. Buzachis, A. Celesti, A. Galletta, M. Fazio, G. Fortino, and M. Villari, "A multi-agent autonomous intersection management (MA-AIM) system for smart cities leveraging Edge-of-Things and blockchain," *Information Sciences*, vol. 522, pp. 148–163, 2020.

[62] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," *IEEE transactions on Industrial informatics*, vol. 7, no. 4, pp. 529–539, 2011.

[63] M. Alazab, S. Khan, S. S. R. Krishnan, Q.-V. Pham, M. P. K. Reddy, and T. R. Gadekallu, "A multidirectional lstm model for predicting the stability of a smart grid," *IEEE Access*, vol. 8, pp. 85 454–85 463, 2020.

[64] A. K. Bashir, S. Khan, B. Prabadevi, N. Deepa, W. S. Alnumay, T. R. Gadekallu, and P. K. R. Maddikunta, "Comparative analysis of machine learning algorithms for prediction of smart grid stability," *International Transactions on Electrical Energy Systems*, vol. 39, no. 9, p. e12706.

[65] Y. Zhang, W. Chen, and W. Gao, "A survey on the development status and challenges of smart grids in main driver countries," *Renewable and Sustainable Energy Reviews*, vol. 79, pp. 137–147, 2017.

[66] Q.-V. Pham, M. Liyanage, N. Deepa, M. VVSS, S. Reddy, P. K. R. Maddikunta, N. Khare, T. R. Gadekallu, W.-J. Hwang *et al.*, "Deep learning for intelligent demand response and smart grids: A comprehensive survey," *arXiv preprint arXiv:2101.08013*, 2021.

[67] A. Jindal, G. S. Aujla, and N. Kumar, "Survivor: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment," *Computer Networks*, vol. 153, pp. 36–48, 2019.

[68] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 43–57, 2019.

[69] J. Wang, L. Wu, K. R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1984–1992, 2020.

[70] R. Vinayakumar, M. Alazab, S. Srinivasan, Q.-V. Pham, S. K. Padannayil, and K. Simran, "A visualized botnet detection system based deep learning for the Internet of Things networks of smart cities," *IEEE Transactions on Industry Applications*, vol. 56, no. 4, pp. 4436–4456, 2020.

[71] D. Nagothu, R. Xu, S. Y. Nikouei, and Y. Chen, "A microservice-enabled architecture for smart surveillance using blockchain technology," in *2018 IEEE International Smart Cities Conference (ISC2)*, Kansas City, Missouri, USA, 2018, pp. 1–4.

[72] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, pp. 18 611–18 621, 2019.

[73] D. Bruneo, S. Distefano, M. Giacobbe, A. L. Minnolo], F. Longo, G. Merlino, D. Mulfari, A. Panarello, G. Patanè, A. Puliafito, C. Puliafito, and N. Tapas, "An IoT service ecosystem for smart cities: The #SmartME project," *Internet of Things*, vol. 5, pp. 12 – 33, 2019.

[74] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Generation Computer Systems*, vol. 86, pp. 650–655, 2018.

[75] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "Privysharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities," *Computers & Security*, vol. 88, p. 101653, 2020.

[76] B. W. Jo, R. M. A. Khan, and Y.-S. Lee, "Hybrid blockchain and Internet-of-Things network for underground structure health monitoring," *Sensors*, vol. 18, no. 12, p. 4268, 2018.

[77] N. Deepa, B. Prabadevi, P. K. Maddikunta, T. R. Gadekallu, T. Baker, M. A. Khan, and U. Tariq, "An AI-based intelligent system for healthcare analysis using Ridge-Adaline stochastic gradient descent classifier," *Journal of Supercomputing*, vol. 77, pp. 1998–2017, 2021.

[78] T. R. Gadekallu, N. Khare, S. Bhattacharya, S. Singh, P. K. R. Maddikunta, and G. Srivastava, "Deep neural networks to predict diabetic retinopathy," *J. Ambient Intell. Humaniz. Comput*, pp. 1–14, 2020.

[79] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and B. Sadoun, "Habits: Blockchain-based telesurgery framework for healthcare 4.0," in *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*. IEEE, 2019, pp. 1–5.

[80] A. Islam and S. Y. Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things," *Computers & Electrical Engineering*, vol. 84, p. 106627, 2020.

[81] R. Ch, G. Srivastava, T. R. Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "Security and privacy of UAV data using blockchain technology," *Journal of Information Security and Applications*, vol. 55, p. 102670, 2020.

[82] M. A. Rahman, M. S. Hossain, G. Loukas, E. Hassanain, S. S. Rahman, M. F. Alhamid, and M. Guizani, "Blockchain-based mobile edge computing framework for secure therapy applications," *IEEE Access*, vol. 6, pp. 72 469–72 478, 2018.

[83] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture," in *2019 IEEE International Conference on Blockchain (Blockchain)*, Atlanta, USA, 2019, pp. 44–51.

[84] M. A. Rahman, E. Hassanain, M. M. Rashid, S. J. Barnes, and M. S. Hossain, "Spatial blockchain-based secure mass screening framework for children with dyslexia," *IEEE Access*, vol. 6, pp. 61 876–61 885, 2018.

[85] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," *Human-centric Computing and Information Sciences*, vol. 10, no. 1, pp. 1–14, 2020.

[86] C. Lin, D. He, N. Kumar, X. Huang, P. Vijaykumar, and K.-K. R. Choo, "Homechain: A blockchain-based secure mutual authentication system for smart homes," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 818–829, 2019.

[87] P. Verma and S. K. Sood, "Fog assisted-IoT enabled patient health monitoring in smart homes," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1789–1796, 2018.

[88] P. Li, C. Xu, H. Jin, C. Hu, Y. Luo, Y. Cao, J. Mathew, and Y. Ma, "ChainSDI: A software-defined infrastructure for regulation-compliant home-based healthcare services secured by blockchains," *IEEE Systems Journal*, vol. 14, no. 2, pp. 2042–2053, 2019.

[89] M. Numan, F. Subhan, W. Z. Khan, S. Hakak, S. Haider, G. T. Reddy, A. Jolfaei, and M. Alazab, "A systematic review on clone node detection in static wireless sensor networks," *IEEE Access*, vol. 8, pp. 65 450–65 461, 2020.

[90] X. Xu, Q. Liu, Y. Luo, K. Peng, X. Zhang, S. Meng, and L. Qi, "A computation offloading method over big data for IoT-enabled cloud-edge computing," *Future Generation Computer Systems*, vol. 95, pp. 522–533, 2019.

[91] N. Tariq, M. Asim, F. Al-Obeidat, M. Zubair Farooqi, T. Baker, M. Hammoudeh, and I. Ghafir, "The security of big data in fog-enabled IoT applications including blockchain: a survey," *Sensors*, vol. 19, no. 8, p. 1788, 2019.

[92] X. Xu, X. Zhang, H. Gao, Y. Xue, L. Qi, and W. Dou, "Become: Blockchain-enabled computation offloading for IoT in mobile edge computing," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4187–4195, 2019.

[93] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[94] A. Singh, R. M. Parizi, Q. Zhang, K.-K. R. Choo, and A. Dehghantanha, "Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities," *Computers & Security*, vol. 88, p. 101654, 2020.

[95] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[96] A. Savelyev, "Copyright in the blockchain era: Promises and challenges," *Computer law & security review*, vol. 34, no. 3, pp. 550–561, 2018.

[97] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K.-K. R. Choo, "Best: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system," *Computers & Security*, vol. 85, pp. 288–299, 2019.

[98] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1972–1983, 2020.

[99] K. Mahmood, X. Li, S. A. Chaudhry, H. Naqvi, S. Kumari, A. K. Sangaiah, and J. J. Rodrigues, "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," *Future Generation Computer Systems*, vol. 88, pp. 491–500, 2018.

[100] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 11, pp. 7081–7093, 2019.

[101] H. Liu, P. Zhang, G. Pu, T. Yang, S. Maharjan, and Y. Zhang, "Blockchain empowered cooperative authentication with data traceability in vehicular edge computing," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4221–4232, 2020.

[102] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Network*, vol. 32, no. 3, pp. 78–83, 2018.

[103] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660–4670, 2018.

[104] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9463–9472, 2020.

[105] D. He, N. Kumar, S. Zeadally, A. Vinel, and L. T. Yang, "Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2411–2419, 2017.

[106] K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, "Differential privacy-based blockchain for industrial internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4156–4165, 2020.

[107] D. He, N. Kumar, and J.-H. Lee, "Privacy-preserving data aggregation scheme against internal attackers in smart grids," *Wireless Networks*, vol. 22, no. 2, pp. 491–502, 2016.

[108] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7992–8004, 2019.

[109] J. Wan, J. Li, M. Imran, and D. Li, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3652–3660, 2019.

[110] G.-Y. Lin, S. He, H. Huang, J.-Y. Wu, and W. Chen, "Access control security model based on behavior in cloud computing environment," *Journal of China Institute of Communications*, vol. 33, no. 3, pp. 59–66, 2012.

[111] C. K. Pyoung and S. J. Baek, "Blockchain of finite-lifetime blocks with applications to edge-based IoT," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2102–2116, 2019.

[112] G. Singh, A. Singh, M. Singh, S. Sharma, N. Kumar, and K.-K. R. Choo, "BloCkEd: blockchain-based secure data processing framework in edge envisioned V2X environment," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5850–5863, 2020.

[113] D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad, and J. Wang, "Blockchain-enabled distributed security framework for next generation IoT: An edge-cloud and software defined network integrated approach," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6143–6149, 2020.

[114] Y. Pu, C. Hu, S. Deng, and A. Alrawais, "Rpeds: A recoverable and revocable privacy-preserving edge data sharing scheme," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8077–8089, 2020.

[115] L. Nkenyereye, B. Adhi Tama, M. K. Shahzad, and Y.-H. Choi, "Secure and blockchain-based emergency driven message protocol for 5G enabled vehicular edge computing," *Sensors*, vol. 20, no. 1, p. 154, 2020.

[116] Y. Dai, D. Xu, K. Zhang, S. Maharjan, and Y. Zhang, "Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4312–4324, 2020.

[117] M. Zhaofeng, W. Xiaochang, D. K. Jain, H. Khan, G. Hongmin, and W. Zhen, "A blockchain-based trusted data management scheme in edge computing," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2013–2021, 2019.

[118] L. Xiao, Y. Ding, D. Jiang, J. Huang, D. Wang, J. Li, and H. V. Poor, "A reinforcement learning and blockchain-based trust mechanism for edge networks," *IEEE Transactions on Communications*, vol. 68, no. 9, pp. 5460–5470, 2020.

[119] L. Cui, S. Yang, Z. Chen, Y. Pan, Z. Ming, and M. Xu, "A decentralized and trusted edge computing platform for Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3910–3922, 2019.

[120] I.-H. Chuang, S.-H. Huang, W.-C. Chao, J.-S. Tsai, and Y.-H. Kuo, "TIDES: A trust-aware IoT data economic system with blockchain-enabled multi-access edge computing," *IEEE Access*, vol. 8, pp. 85 839–85 855, 2020.

[121] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: review and challenges," *IEEE Access*, vol. 7, pp. 164 908–164 940, 2019.

[122] M. Moniruzzaman, S. Khezr, A. Yassine, and R. Benlamri, "Blockchain for smart homes: Review of current trends and research challenges," *Computers & Electrical Engineering*, vol. 83, p. 106585, 2020.

[123] X. Xu, Z. Zeng, S. Yang, and H. Shao, "A novel blockchain framework for industrial IoT edge computing," *Sensors*, vol. 20, no. 7, p. 2061, 2020.

[124] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 858–880, 2018.

[125] U. Jayasinghe, G. M. Lee, Á. MacDermott, and W. S. Rhee, "Trustchain: a privacy preserving blockchain with edge computing," *Wireless Communications and Mobile Computing*, vol. 2019, pp. 1–17, 2019.

[126] V. Gramoli and M. Staples, "Blockchain standard: Can we reach consensus?" *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 16–21, 2018.

[127] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2018.

[128] C. Xu, K. Wang, and M. Guo, "Intelligent resource management in blockchain-based cloud datacenters," *IEEE Cloud Computing*, vol. 4, no. 6, pp. 50–59, 2017.

[129] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, 2018.

[130] M. Samaniego and R. Deters, "Hosting virtual IoT resources on edge-hosts with blockchain," in *2016 IEEE International Conference on Computer and Information Technology (CIT)*. IEEE, 2016, pp. 116–119.

[131] O. Novo, "Scalable access management in IoT using blockchain: a performance evaluation," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4694–4701, 2018.

[132] J. Pan, J. Wang, A. Hester, I. AlQerm, Y. Liu, and Y. Zhao, "Edgechain: An edge-IoT framework and prototype based on blockchain and smart contracts," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4719–4732, 2018.

[133] M. Alamri, N. Jhanjhi, and M. Humayun, "Blockchain for Internet of Things (IoT) research issues challenges & future directions: A review." *Int. J. Comput. Sci. Netw. Secur*, vol. 19, pp. 244–258, 2019.

[134] D. C. Nguyen, P. Cheng, M. Ding, D. Lopez-Perez, P. N. Pathirana, J. Li, A. Seneviratne, Y. Li, and H. V. Poor, "Enabling AI in Future Wireless Networks: A Data Life Cycle Perspective," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 553–595, 2020.

[135] S. Russell and P. Norvig, *Artificial intelligence: a modern approach*. Prentice hall, 2002.

[136] A. Nawaz, T. Gia, J. P. Queralta, and T. Westerlund, "Edge AI and blockchain for privacy-critical and data-sensitive applications," in *2019 Twelfth International Conference on Mobile Computing and Ubiquitous Network (ICMU)*. IEEE, 2019, pp. 1–2.

[137] J. Xu, S. Wang, A. Zhou, and F. Yang, "Edgence: A blockchain-enabled edge-computing platform for intelligent iot-based dapps," *China Communications*, vol. 17, no. 4, pp. 78–87, 2020.

[138] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

[139] X. Wang, Y. Han, C. Wang, Q. Zhao, X. Chen, and M. Chen, "In-edge AI: Intelligentizing mobile edge computing, caching and communication by federated learning," *IEEE Network*, vol. 33, no. 5, pp. 156–165, 2019.

[140] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making knowledge tradable in edge-AI enabled IoT: A consortium blockchain-based efficient and incentive approach," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6367–6378, 2019.

[141] A. Chaer, K. Salah, C. Lima, P. P. Ray, and T. Sheltami, "Blockchain for 5G: opportunities and challenges," in *2019 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2019, pp. 1–6.

[142] E. Chang, K. Y. Chan, P. Clark, and V. Potdar, "Guest editorial: Blockchain and AI enabled 5G mobile edge computing," *IEEE Transactions on Industrial Informatics*, 2020.

[143] K. Zhang, Y. Zhu, S. Maharjan, and Y. Zhang, "Edge intelligence and blockchain empowered 5G beyond for the industrial Internet of Things," *IEEE Network*, vol. 33, no. 5, pp. 12–19, 2019.

[144] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-vanets," *IEEE Access*, vol. 7, pp. 56 656–56 666, 2019.

[145] H. Yang, Y. Liang, J. Yuan, Q. Yao, A. Yu, and J. Zhang, "Distributed blockchain-based trusted multi-domain collaboration for mobile edge computing in 5G and beyond," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 11, pp. 7094–7104, 2020.

[146] F. Miatton, "Blockchain at the edge: The nexus of capturing new value in 5G," in *2020 International Conference on Technology and Entrepreneurship - Virtual (ICTE-V)*. IEEE, 2020, pp. 1–6.