Ann. For. Res. 65(1): 3888-3900, 2022
ISSN: 18448135, 20652445

ANNALS OF FOREST RESEARCH
https://www.e-afr.org/

INTELLIGENT IOT COMMUNICATION SYSTEM BASED ON BLOCK CHAIN

Mr. S. Premkumar[1], Dr.Manikannan Kaliyaperumal[2], Mrs.A.Abirami[3], Ms.S.Bhuvaneswari[4] , Dillip Narayan Sahu[5*], Idamakanti Kasireddy[6]

[1]Assistant Professor, Department of Computer Science Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India.

[2]Associate professor Gr ll, Department of Computer Science and Engineering, RMK Engineering College, Kavaraipettai, Tamil Nadu, India.

[3]Assistant Professor, Department of Computer Science and Engineering, Easwari Engineering College (Autonomous), Chennai, Tamilnadu, India.

[4]Assistant professor, Department of CSE, Easwari Engineering College, Chennai, Tamilnadu, India.

[5*]Assistant Professor, Department of MCA, Gangadhar Meher University, Odisha, India.

[6]Associate Professor, EEE Department, Vishnu Institute of Technology Bhimavaram, AP, India.

Corresponding Author Email-id: Dillip1seminar@gmail.com

Abstract

Communication will soon enter a new age ushered in by the Internet of Things (IoT). With the use of IoT, inanimate things may be given the ability to generate, receive, and share information with one another. High levels of security, privacy, authentication, and recovery from assaults are necessary to create such a society in an expanding manner. In this light, modifying the design of IoT applications is crucial for establishing fully protected IoT ecosystems. In this paper, we will examine the issues surrounding security in the Internet of Things and provide solutions. Multiple Distributed Ledger Technologies (DLTs) are proposed for usage in distinct Internet of Things (IoT) settings. The suggested security methods are generalised to account for the wide variety of IoT use cases. Blockchain facilitates the development of a decentralised network in which nodes or peers are dispersed across space and time and do not have any prior relationship with or mutual trust among one another. While blockchain has shown promise in the financial and e-commerce sectors, its direct use in other industries is not yet possible. Generic blockchains have severe shortcomings in key areas; they include scalability, efficiency, transaction sequencing, microtransaction capacity, and more. The study as a whole provides computationally efficient consensus methods and application-based smart contracts for vehicular, mobile, and aerial drone peer-to-peer networks.

Keywords: Internet of Things (IoT), Blockchain , algorithm, peer -to-peer and security.

1. Introduction

The pace at which we are able to link the world's physical things to the Internet is expanding exponentially. There will be over 8.4 billion connected gadgets in use throughout the globe by 2020, according to a recent forecast by Gartner [1]. The research predicts a rise of 20.4, billion by 2022 [2]. The adoption of Internet of Things applications is rising rapidly throughout the globe, especially in nations like China, Western Europe, and North America [3]. From 5.6 billion in 2016,

the number of Internet-connected devices and the amount of communication between them is projected to rise to 27,000,000,000 by 2024 [3]. Also, between 2018 and 2025 [4,] the IoT market is projected to expand from $892 billion to $4 trillion in revenue. The exponential growth in these statistics proves that the Internet of Things is one of the most promising emerging sectors in the near future [5]. Figure.1 depicts the evolution of the Internet of Things from its inception to the present day. All gadgets will eventually have internet access and communicate with one another via peer-to-peer protocols, as seen in the image. Social Internet of Things (SIoT) is another up-and-coming idea that may link people from various social networks to the gadgets [6]. The proliferation of IoT applications that aim to improve the lives of the masses comes with a number of serious privacy and security risks. If an open and reliable ecosystem is not in place, the developing IoT applications will fail to inspire widespread adoption and may never realise their full potential. Security challenges unique to the Internet of Things include authentication, data management, and privacy protection. Security and privacy threats have been made against the presently deployed IoT applications all around the globe. Since IoT devices tend to be insecure and underpowered, they make it simple for cybercriminals to breach business networks and obtain access to sensitive user information. About 2.5 million devices were compromised and DDoS assaults were initiated in the fourth quarter of 2016 due to the Mirai attack [7]. Devices connected to the Internet of Things have also been successfully placed in the bodies of live individuals, such as patients, to monitor various conditions including heart problems [8]. In spite of this, such IoT apps might make it possible for attackers to monitor the movements of a specific individual, which can be especially dangerous if the target is a public figure with significant sway. A breach of these devices may be very risky, and there are yet no instances of such efforts.

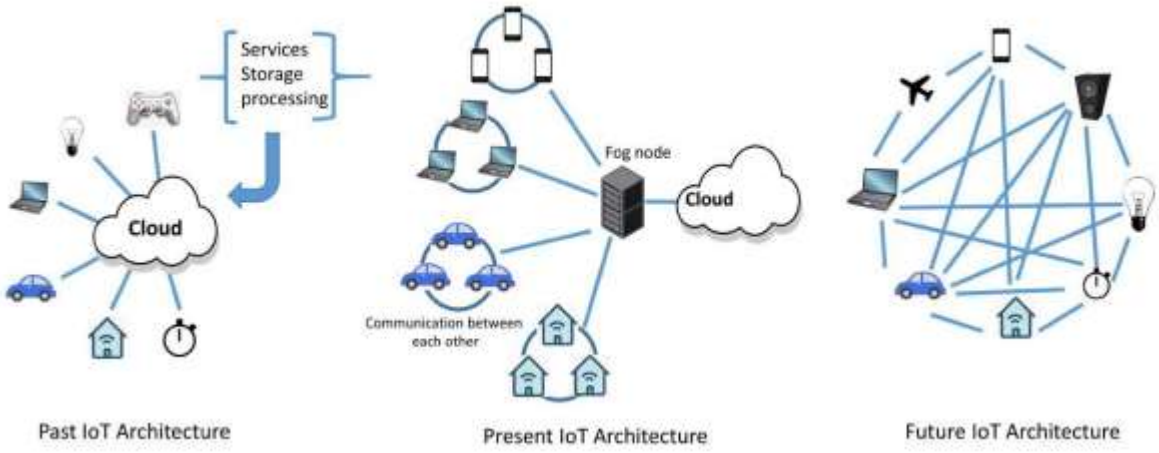

Figure.1. Difference Between the Previous, Current, and Futuristic Architecture of IoT.

Cyber-physical systems are another area that stands to benefit from the expansion of the Internet of Things (CPS). Connected physical systems (CPS) use the internet to react to physical changes by interacting with the things and items already existing at a location via the use of sensors. There are severe repercussions in security vulnerabilities due to the fact that CPS is linked to very essential applications (such as automobile networks, mobile networks, and the internet of drones).

There are four crucial levels in each Internet of Things ecosystem. Actuators and sensors in the first layer process the data or information for use in the system's other processes. The information is sent along through a communication network in the second layer, which is based on the first [9]. New applications for the Internet of Things will have a third layer, often referred to as the middleware layer. It bridges the gap between the application and the network layer. Applications like smart houses, smart metres, smart automobiles, and so on make up the last layer. In addition to the aforementioned four levels, several other entry points exist. Concerns about data safety are not limited to these entry points.

2. Securing IoT Using Blockchain

When combined, the Internet of Things and blockchain are two groundbreaking technologies that might significantly alter the information technology and communications landscape [10]. These innovations seek to make life easier for their end users by increasing clarity, openness, trust, and convenience. Blockchain's underlying concept is simple: it's just a distributed ledger, or a set of duplicated log files. In a blockchain, transactions are recorded in chronological order along with timestamps. A cryptographic hash key is used to link each ledger entry inextricably to the one before it. Figure.2 is an example of the architecture of a blockchain and the method in which each block is linked to all of the preceding blocks using cryptographic hashing. Each individual transaction is recorded in a Merkle tree, and the hash of the tree's root is kept in the blockchain. Cryptographically hashed versions of these transactions (denoted Ha, Hb, Hc,...) are stored in the tree's leaf nodes. By joining the hashes of the child nodes, a new root hash is generated [11]. The blockchain keeps a record of the ultimate root hash (H1, H2,...). If even one transaction on one branch of the tree is updated, all the hash values on that branch will also be changed. Therefore, it is sufficient to check the root hash to ensure the integrity and safety of all connected transactions. The miner or ledger keeper checks the logs or transactions and generates a key so that the most recent transaction may be added to the whole ledger. This method ensures that the most recent data is distributed to all network nodes. The existence of cryptographic hash keys in each block makes it very difficult and time consuming for attackers to tamper with any data contained inside [12].

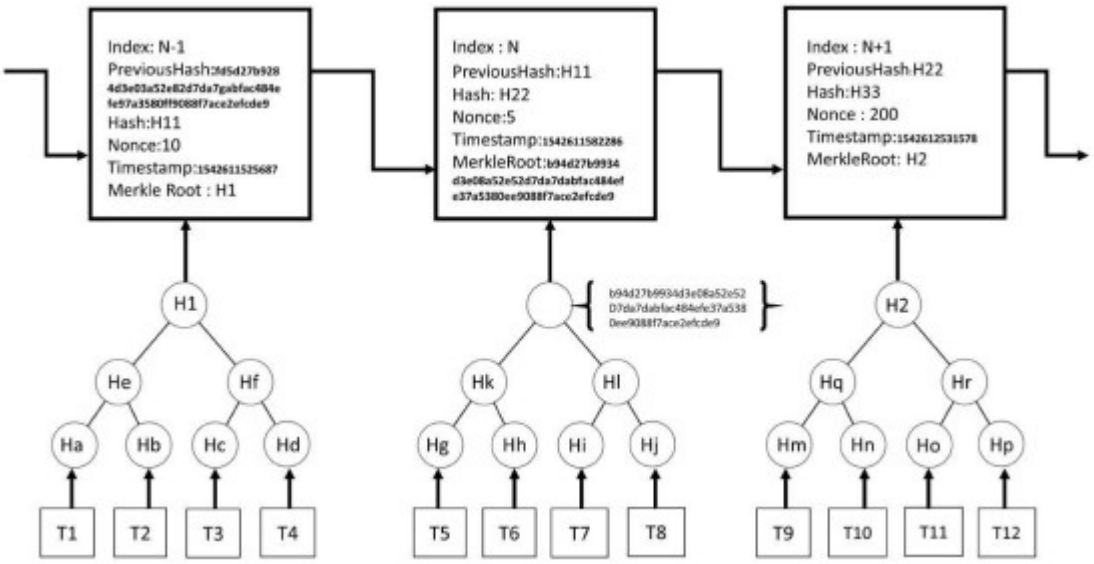

Figure.2. Basic Blockchain Architecture.

The blockchain's special properties make it an ideal distributed, secure, and publicly accessible data structure for IoT information [13]. The miners are just interested in the rewards they may get from their efforts; they have no stake in the underlying cryptocurrency itself. Furthermore, the miners do not know who the actual transaction owners are. In addition, several miners are simultaneously processing the same group of transactions, and they are in fierce rivalry with one another to be the first to add those transactions to the blockchain.

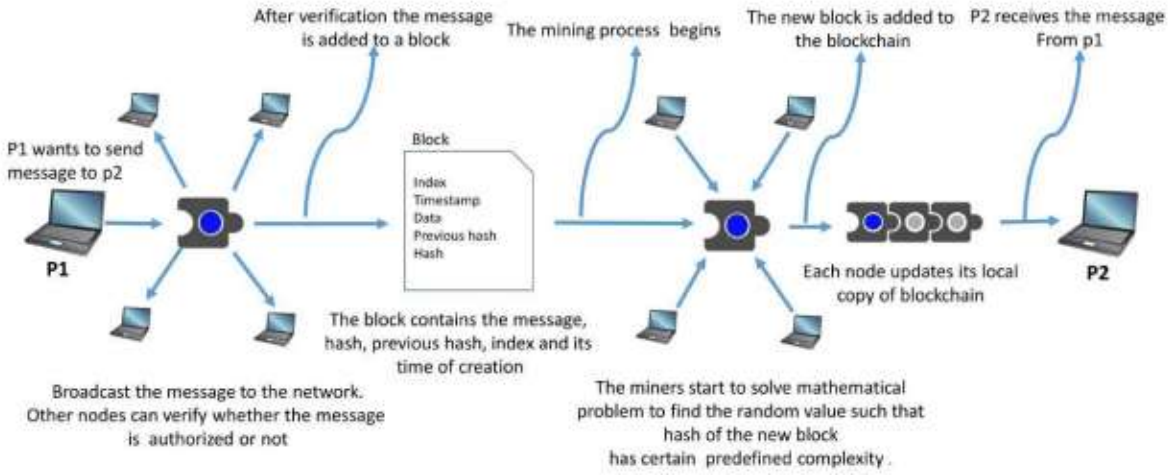

Figure.3. Working process of Blockchain.

Figure.3 depicts the whole lifecycle of a transaction, from its inception to its subsequent commit to the distributed ledger. Different blockchain creation and maintenance frameworks and platforms are under active development in both academic and industry. Ripple, Ethereum, Hyperledgerfabric, etc. are all instances of such systems [14].

3. Literature Survey

Concerns unique to each IoT environment layer are addressed here. As a follow-up to our discussion of the problems plaguing IoT applications, we will now move on to the basic upgrades and advancements needed for the next generation of IoT apps. Then, we show the current state of the art in certain crucial areas of VANET, MANET, and IoD-related applications. Details on the strengths, weaknesses, and potential applications of these works are also provided. We also cover the background research that led to the development of a novel distributed network and consensus method used in this paper.

When developing an IoT application, it's important to keep in mind that the usage of many technologies at different layers increases the likelihood of security vulnerabilities. Devices, applications, and technology at each of these 4 levels are shown in Figure.4. Attacks on each of these four tiers are shown in Figure.5. In addition, the unique security concerns of gateways across layers are discussed here.

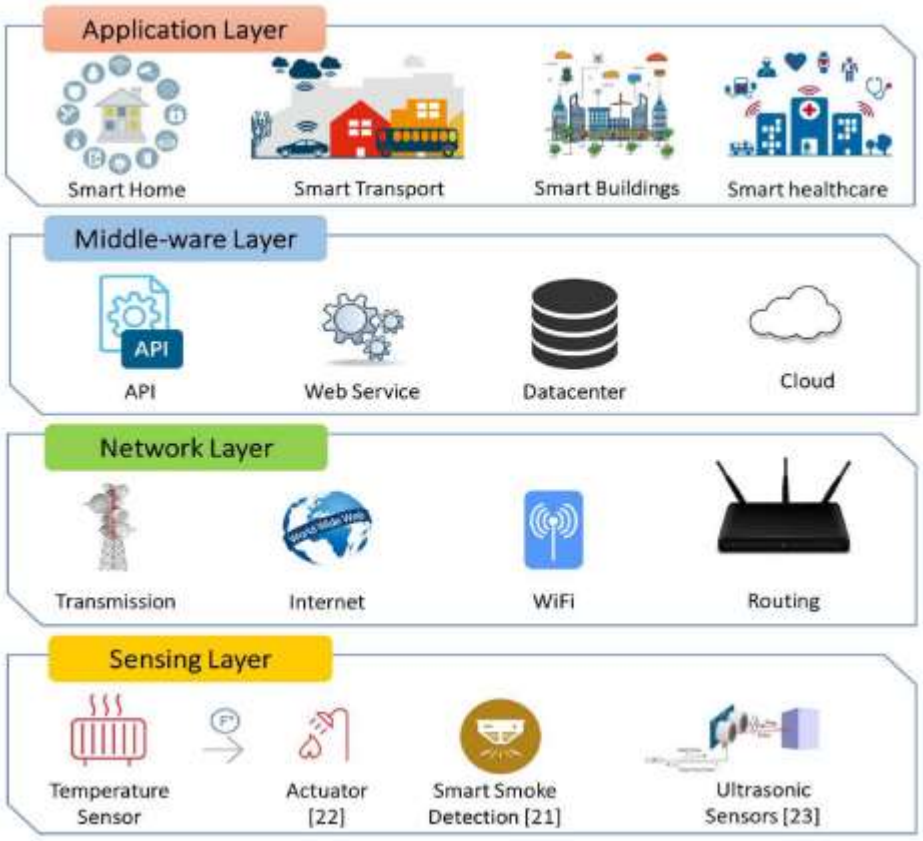

Figure.4. Various Layers in the IoT System.

Sensors pick up on the occurrence of physical phenomena [15]. There are a wide variety of sensors available for gathering a wide variety of information; they include temperature, camera, ultrasonic, and many more. Numerous types of sensors, such as electrical, electronic, mechanical, and chemical, can be used to gather data about the surrounding physical world. Different Internet of

Things applications make use of different sensing layer technologies, such as global positioning systems, radio frequency identification, regional sensor networks, wireless sensor networks, etc.

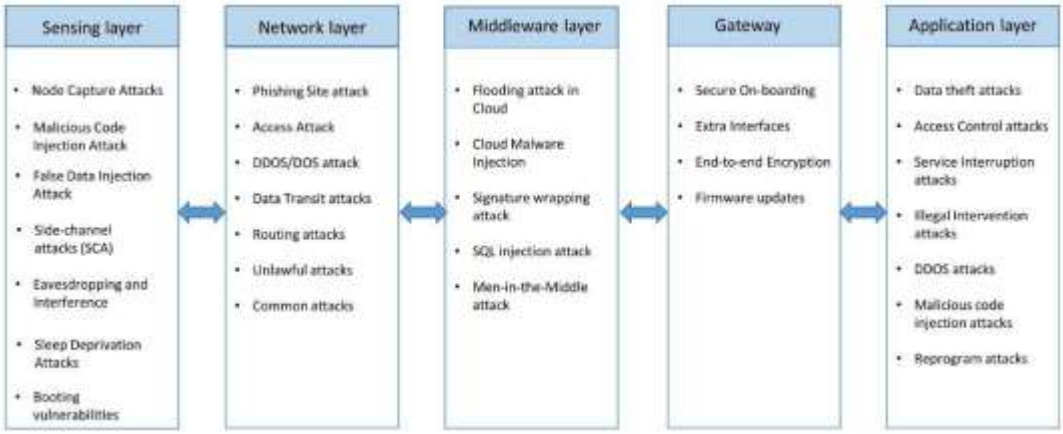

Figure.5. Types of Attacks on IoT.

Firewalls, address space randomization, anti-virus software, and other safeguards are only some of the features standard on smartphones and PCs. Many of the currently available IoT devices lack the aforementioned protective measures. The security issues of IoT devices have not yet been addressed by a well-defined framework that can be utilised for an end-to-end application. An Internet of Things application is a finished good that is the result of teamwork across several sectors and many people. From the sensors to the application, and even down to the edge nodes, where several actuators and sensors are deployed, many different technologies and products are in use. There must be some kind of handshake mechanism between different types of wireless networking protocols [16]. Furthermore, IoT applications utilise a number of different communication technologies at various layers, and we can't just use the ubiquitous HTTP protocol at the application level since it's too cumbersome. As a result of its high parsing overhead, it is unsuitable for usage in contexts with limited computing power. That's why several different protocols have been implemented at the application level for IoT settings. Javascript IoT, Constrained Application Protocol, Message Queuing Telemetry Transport Protocol (MQTT), Simple Message Queuing Telemetry Transport Protocol (SMQTT), M3DA, Advanced Message Queuing Protocol (AMQP), XMPP, etc. IoT applications need trade-offs between security, cost-effectiveness, dependability, latency, privacy, coverage, and so on due to the variety of technologies, devices, and protocols involved. If one measure for improvement is maximised, it may have a negative impact on the other. Connected domains, devices, regions, and technologies form a lengthy chain in a typical IoT application. The durability of a chain is proportional to the weakest link in it. A significant number of weak connections have been seen in modern IoT systems, which may lead to a security risk for the whole programme. Several simple Internet of Things applications, such as smart door locks, may be exploited as weak links to steal a user's WiFi password [17]. The user-data produced everyday by IoT apps might include a wide variety of sensitive information that could be used to harm the system [18]. Therefore, major improvements to the current IoT architecture are needed to make it safe, resilient, and dependable. Most of the apps and services in use today may be classified as either centrally or distributedly

managed. Single point of failure, distributed denial of service attack, high danger of data theft and high risk of central server hacking, lack of scalability, etc. are all problems that arise from a centrally located system. As a result of these systemic flaws in traditional, centralised design models, cutting-edge apps are increasingly adopting decentralised systems like blockchain. Here are some of the most fundamental aspects of blockchain technology that set it apart from traditional centralised systems. Despite the paradigm change from centralised to decentralised application architectures, security solutions continue to be headquartered in a single location. Centralized security methods are inefficient when used to distributed applications. Since blockchain facilitates distributed application security, it works well with the emerging software. This study presents a comprehensive literature review that demonstrates how adopting DLTs is a very promising method for achieving security in many IoT areas. While everyone agrees that DLTs should be used for security, the issue of which DLT should be used in which situation remains open. Numerous distributed ledger technologies (DLTs) and cryptocurrencies are making their debuts in academia and business. Each DLT has its own unique set of capabilities, data formats, and benefits and drawbacks. Blockchain is the most well-known DLT, yet it has a number of severe drawbacks that have yet to be addressed. There were a number of holes in previous research that were addressed here. While generic blockchain is helping to tackle problems like fraud and security, many more remain. There is a close relationship between the blockchain in its general form and monetary and banking systems. A more universal use of blockchain technology inside the Internet of Things will need further refinement of the data format and/or algorithms underlying the technology. Generic blockchian does not keep track of transactional order. There is a discrepancy between the order in which new transactions are introduced to the network and the order in which they are processed. While this probably won't be a problem for everyday banking transactions when the account balance simply stays the same, it might be a problem for applications where resources are scarce and given out on a first-come, first-served basis. Proof of work is a resource-intensive process used in general blockchains; as a result, the Bitcoin blockchain is transitioning away from PoW in favour of proof-of-stake or proof-of-belief. The use of these algorithms to mine blocks requires the expenditure of certain coins. When these algorithms are successfully mined, the miners are rewarded with a portion of the transaction fees. It's possible that these algorithms might be useful in more broad financial applications, but they wouldn't be practical for microtransactions. In mobile ad hoc networks (MANETs), for instance, there are too many microtransactions for the general blockchain to be useful. A mobile user may send a request for a snippet of information to another mobile, and the latter may choose to charge a tiny fee, denominated in micro tokens, for providing the requested information. Such transactions cannot be fulfilled using traditional blockchain, as the mining fees will end up to be more than the actual transaction cost.

4. Digital Identity

The authors of this piece introduce a decentralised network of parking-lot owners and drivers. When a driver connects to a network, a pair of private and public keys is produced for it using an elliptic curve digital signature application (ECDSA). The secret cypher d is a huge string of random digits generated by a computer programme. Every transaction that takes place between

the nodes of the network makes use of this set of keys to prevent the problem of non-repudiation and guarantee there is no confusion about the allocation. It is the responsibility of the issuing party to digitally sign the transaction with the private key, while the other nodes may verify the message using the signing authority's public key. User requests for parking spots may be made after keys have been created. Before the allocation, the user must fill out a form with information about the location, the time and length of the slot needed, the maximum amount the user is prepared to pay, and so on. Next, the information is placed in a transaction container and sent out to the network's nodes. An example of the event framework is shown in Figure.6. Because the gossip protocol requires much less bandwidth to gossip the DAG that it generates, and because the users "gossip the gossip," the network's reach grows dramatically, all of this takes place in the form of a gossip event. The next part of this article discusses how create gossip-based schedule and assign parking spots. The parking reservation request is analogous to a blockchain transaction, and the event is synonymous with a block. Figure 6 illustrates how several slot booking requests may be made for a single event or block. There are many parking slot requests associated with each event in the graph, including the current parking slot request made by the user and some past requests that have not yet achieved a consensus and are flowing via the gossip protocol.

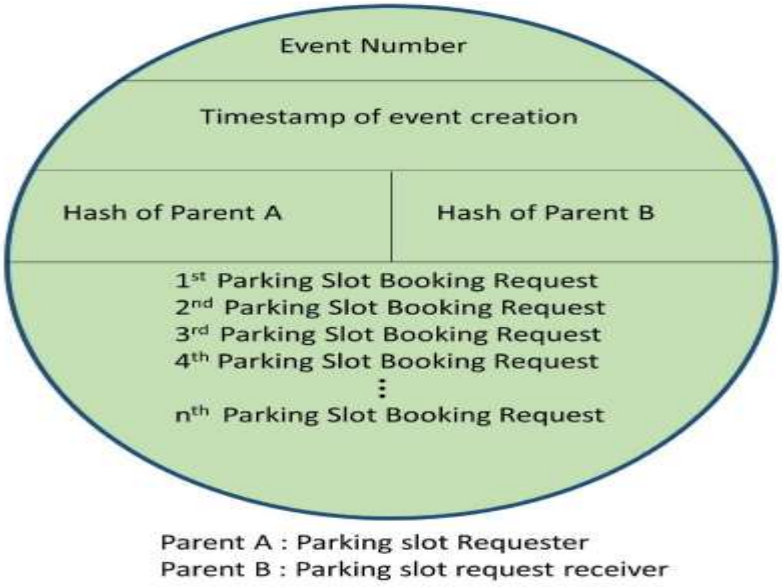

Figure.6. Architecture of event created in DAG

Consensus algorithms are a crucial component of any distributed ledger technology (DLT) or distributed application (Dapp) since they establish credibility and credibility amongst previously untrusted network participants. Several popular consensus algorithms, such as Raft and Paxos, achieve consensus through appointing a leader to act as mediator between the nodes in the network. This is necessary since there is no centralised entity in a distributed framework to bring all the nodes to an accord. Consensus algorithms, however, are very vulnerable to denial-of-service (DOS) assaults and endless delays. Threats against even a single node in a network may have far-reaching effects. The POW (proof-of-work) technique is employed in

an open distributed network to tame the aforementioned difficulties and come to an agreement. The POW method enables the blocks to be added at the node that requires the least amount of time to solve a random mathematical puzzle. There are, however, certain considerations that should be made while using the generic POW method. One problem is that adding a block causes an increase in overall power consumption owing to the introduction of new delay. Second, this approach does not provide finality since a transaction or communication added to a block may be withdrawn at a later time. Additionally, the POW algorithm does not keep a properly ordered record of communications; there is no correlation suggesting a relationship in the order in which transactions enter a network and are performed. Keeping a well-ordered record of transactions may not seem necessary when dealing with the POW algorithm, which is primarily used in bitcoin, but it is crucial when dealing with a smart parking scheduling and allocation system, where the number of users and the number of parking slots are disproportionate. As a result, it's crucial to think about the booking slots' availability and assign them to users properly. The proof-of-expired-time (POET) method exemplifies a means to achieve the efficiency and competency of POW without the need of power overhead. This method avoids wasteful use of resources but comes at the expense of user confidence. The Byzantine agreement mechanism attempts to address this problem by considering member votes. While these systems are great at winning over users, they often suffer from a significant message transmission overhead on the scale of O(n), O(n 2), or even O(n 3). The aforementioned problems are inherent to the general consensus method, hence a DAG-based agreement algorithm is developed to address them. This method has been shown to be efficient, quick, and deterministic while preventing any genuine block from becoming a fork, giving all the benefits of blockchain technology. Every miner has the power to mine new blocks, and all mined blocks are added to the main chain without the need to spend additional time and resources on calculation of challenging mathematical challenges. This algorithm utilises the principle of electronic voting to prevent unnecessary communication. Online voting eliminates the need for voters to interact with each other. It's true that until proof of work has been used for a significant amount of time, a new consensus method cannot be applied to a brand new chain. This is due to the fact that the quantity of cryptocurrency held by each user affects the outcome of other supporting algorithms like proof of burn and proof of stake. Because the network is very new, there is currently no coin in circulation and hence no users. For this reason, it makes no sense to risk anything in a proof of stake scenario or waste any bitcoin in a proof of burn scenario. However, the suggested consensus method does not function as a proof-of-work auxiliary algorithm. The suggested method is completely decentralised and does not rely on any central authority or centralised database. The suggested model relies on the graph generated by the gossip protocol and performs well both at the outset and later in the life of the blockchain. Therefore, the proposed algorithms can be applied to both the existing applications as well as the new orfreshly started Dapps.

5. Results and Discussion

Figure.7 displays the wide range of parking rates charged by various parking lot proprietors. In a variety of locations, users may book parking spots ahead of time. Assuming that User 1 and User 2 want to book parking spots in Lots 1 and 2, respectively. It turns out that parking costs are inversely proportional to the distance between the user's final destination and the parking lot. The greater the distance, the cheaper the fare. Looking at Figure.8 reveals a consistent pattern between weekday and holiday pricing. It has been noted that during festival days, parking fees are often higher than they normally would be at most parking lots.

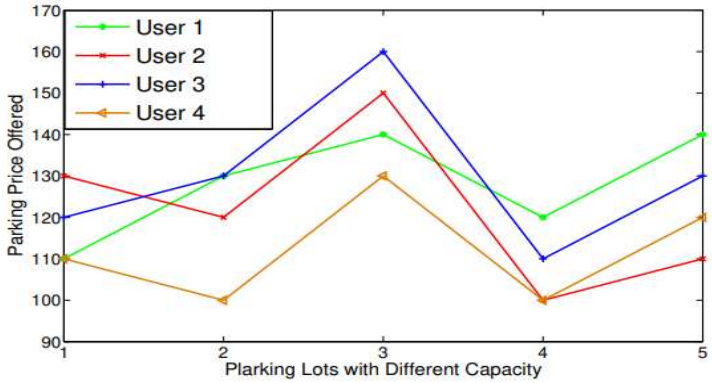

Figure.7. Variation of Prices to Different Users by Different Parking Lots on a NonFestival day.

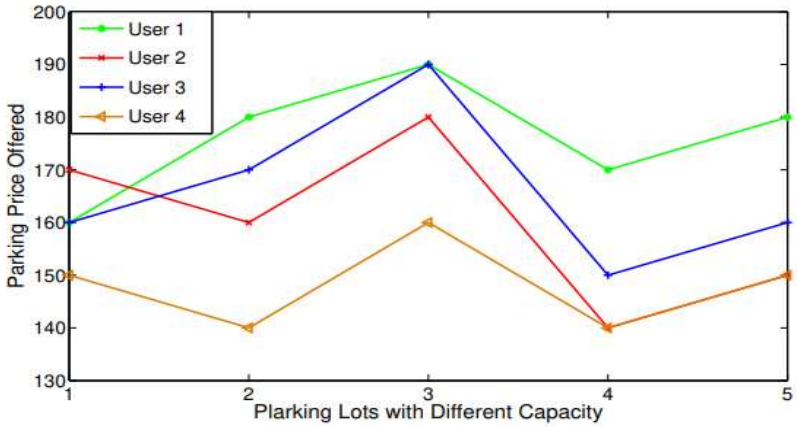

Figure.8. Variation of Prices to Different Users by Different Parking Lots on a Festival day.

Parking space resource usage rates are shown in Figure 9 and Figure 10 when the suggested model is not in use and when it is in use, respectively. Users of the model, when it is not in use, have a tendency to park their cars in the largest available spots, resulting in traffic congestion and the underutilization of parking lots even during rush hours. Users still have to circle the expansive parking lots in quest of an open place, despite the exorbitant prices they pay. The suggested approach facilitates this process by providing a vacant slot in response to the user's requests and do so at a lesser price in most circumstances. Users and landowners alike may save time and energy as a result of this development. Users pay the lowest possible rates for the best available parking, while lot owners see their lots put to good use. Figure.10

shows that the largest lot has a utilisation rate that is almost the same as the other four lots, but the other two lots both show a significant increase in their usage. Increasing the incentive for private property owners and operators of small parking lots to provide parking spaces would benefit greatly from an increase in the efficiency with which these resources are used. It will gradually enhance parking alternatives for users, which will decrease the likelihood of traffic jams. The most important takeaway from these two numbers is that the proposed model has improved the resource utilisation of the small parking lots without affecting the resource utilisation of the larger parking lots, which were already available to all users. This demonstrates that some customers were having a hard time locating a parking space in the larger parking lots because they were not aware of the smaller parking lots in the immediate area. As a result, the suggested model is advantageous not only for regular customers but also for parking lot proprietors.

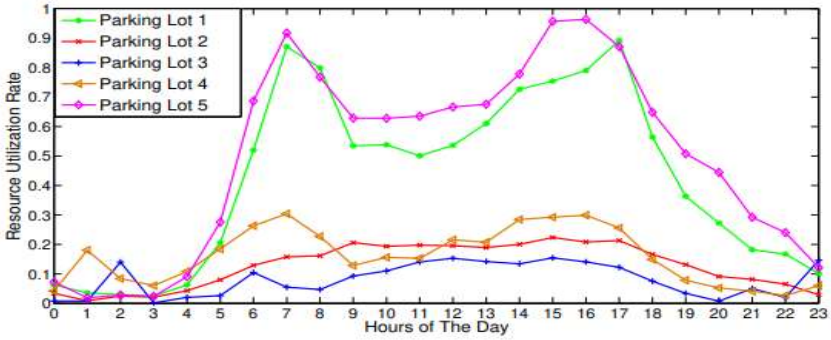

Figure.9. Rate of Resource Utilization for different PLs Without Proposed Model.

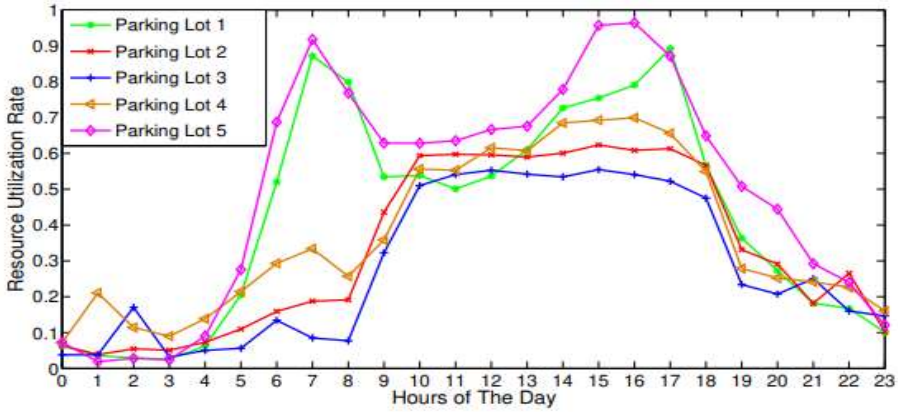

Figure.10. Rate of Resource Utilization for different PLs With Proposed Model.

6. Conclusion

Many Internet of Things (IoT) cloud-based applications have a weak spot: they rely on a single service or component. Blockchain technology eliminates the need for a centralised server, hence this problem is moot. As long as there is an accessible blockchain, the information created by the devices may be simply and securely stored, regardless of their physical location. With the use of distributed ledger technology, we can build a trustworthy peer-to-peer network connecting all the people involved in the parking industry from lot and garage owners to drivers in need of parking

to those with open spots to share. By listing their spots on the platform, parking lot owners have access to potential customers and potential revenue streams. By assigning distinct consensus timestamps to each service request, the directed acyclic graph assures that consumers get service that is both efficient and affordable. We spoke about a dynamic pricing approach that would be good for parking lot owners and customers alike by offering personalised rates in response to each parking request. Users may save time and money thanks to this approach, while parking lot owners can benefit from fuller usage of their spots. Simulation findings corroborate the effectiveness of the suggested approach in avoiding bottlenecks, shortening users' search times, and making the most of available resources. Increasing the incentive for private property owners and operators of small parking lots to provide parking spaces would benefit greatly from enhanced resource use. If this is implemented, there will be more parking spots available for users, which will decrease the likelihood of traffic congestion.

References

1. Gsma , "Safety, privacy and security," https://www.gsma.com/publicpolicy/ resources/safety-privacy-security-across-mobile-ecosystem/, online; accessed October. 25, 2018.
2. Flashpoint , "Mirai Botnet Linked to Dyn DNS DDoS Attacks," https://www.flashpoint-intel.com/blog/cybercrime/mirai-botnet-linkeddyn-dns-ddos-attacks/, online; December. 18 ,2018.
3. Yang G. , Jiang M. , Ouyang W. , Ji G. , Xie H. , Rahmani A. M. , Liljeberg P. , and Tenhunen H. , "Iot-based remote pain monitoring system: From device to cloud platform," IEEE journal of biomedical and health informatics, vol. 22, no. 6, pp. 1711–1719, 2018.
4. Hassija V. , Batra S. , Chamola V. , Anand T. , Goyal P. , Goyal N. , and Guizani M. , "A blockchain and deep neural networks-based secure framework for enhanced crop protection," Ad Hoc Networks, vol. 119, p. 102537, 2021.
5. Novo O. , "Blockchain meets iot: An architecture for scalable access management in iot," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184–1195, April 2018.
6. Javaid U. , Aman M. N. , and Sikdar B. , "Blockpro: Blockchain based data provenance and integrity for secure iot environments," in Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems. ACM, 2018, pp. 13–18.
7. Javaid U. , Siang A. K. , Aman M. N. , and Sikdar B. , "Mitigating lot device based ddos attacks using blockchain," in Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems. ACM, pp. 71–76, 2018.
8. Ozyilmaz K. R. and Yurdakul A. , "Designing a blockchain-based iot with ethereum, swarm, and lora: The software solution to create high availability with minimal security risks," IEEE Consumer Electronics Magazine, vol. 8, no. 2, pp. 28–34, March 2019.
9. Sharma V. , "An energy-efficient transaction model for the blockchain-enabled internet of vehicles (iov)," IEEE Communications Letters, vol. 23, no. 2, pp. 246–249, Feb 2019.

10. Javaid U. , Aman M. N. , and Sikdar B. , "Drivman: Driving trust management and data sharing in vanets with blockchain and smart contracts," in Proceedings ofIEEE Vehicular Technology Conference.IEEE, pp. 1–6, 2019.
11. He D. , Chan S. , and Guizani M. , "Security in the internet of things supported by mobile edge computing," IEEE Communications Magazine, vol. 56, no. 8, pp. 56–61, 2018.
12. Alphand O. , Amoretti M. , Claeys T. , Dall'Asta S. , Duda A. , Ferrari G. , Rousseau F. , Tourancheau B. , Veltri L. , and Zanichelli F. , "Iotchain: A blockchain security architecture for the internet of things," in 2018 IEEE Wireless Communications and Networking Conference (WCNC).IEEE, pp. 1–6, 2018
13. Hassija V. , Gupta V. , Garg S. , and Chamola V. , "Traffic jam probability estimation based on blockchain and deep neural networks," IEEE Transactions on Intelligent Transportation Systems, pp. 1–10, 2020.
14. Alladi T. , Chamola V. , Sikdar B. , and Choo K. R. , "Consumer IoT: Security vulnerability case studies and solutions," IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 17–25, 2020.
15. Alladi T. , Chamola V. , Parizi R. M. , and Choo K.-K. R. , "Blockchain applications for industry 4.0 and industrial IoT: A review," IEEE Access, vol. 7, pp. 176 935–176 951, 2019.
16. Praveen G. , Chamola V. , Hassija V. , and Kumar N. , "Blockchain for 5G: A prelude to future telecommunication," IEEE Networks, 2020.