A Survey on Existing Trends in Integration of Blockchain Technology into Internet of Things

Harshit Agrawal, Sahana P Shankar, Aditi Pal, Akash Sikarwar

Faculty of Engineering and Technology, M.S. Ramaiah University of Applied Sciences, Bangalore 560054

*Contact Author e-mail: sahana.cs.et@msruas.ac.in

Abstract

With the introduction and evolution of internet it gave rise to a separate world called digital world. In age of digital world in which almost everything from a person's social information to their deepest secrets from oldest movies released to latest ones, information about anyone and anything is available on internet. Along with this evolutionary digital world comes concept of digital ownership, which can either be owning a social media account or crypto-currency to name a few. Even most sensitive data such as patient's health records are stored in a central system of hospital which can be hacked and misused. This raises another question of ways of keeping our identities safe. With various privileges that we enjoy with emergence of this digital world we are also losing our privacy completely. In today's world various companies know every single detail about us from every penny spent by us using online bank transactions to every movement of ours using GPS. One possible solution to all above questions can be blockchain technology.

KeyWords: blockchain, security, IoT

1. INTRODUCTION

We all have at least once owned something digitally like a social media account, healthcare records, votes or at least heard about these. All these digital ownerships are implemented on the top of blockchain technology. It can be viewed as an account ledger storing information about the transactions. At its very basic as the name suggests, blockchain is chain of blocks (data) only. Where each block stores some digital data. But having so simple structure, how blockchain plays a critical role in securing the data? Each block in a blockchain is made up combining various pieces of digital information (3 specifically):

1. The first piece of information that every block in the blockchain contains is the basic details about the transaction, which includes time, day, date etc. Also, the amount of the transaction along with the currency type is stored in the block itself. These transactions can be of anything, like movie booking, online shopping, newsletter subscriptions etc. For a better understanding, let's consider the movie booking transaction. So, the block will store the date, day, time and the amount you paid to book the movie.

2. The second piece of information that every block in the blockchain contains is the information about the organization(s) or individual(s) doing and receiving the transaction. Continuing the above movie booking example only, the block stores the name of portal you are booking the movie from (moviebook.com, Inc.). Also, it stores information about the person who's booking the movie. But, since storing the name and details about an individual can be a security concern afterwards, a digital signature (usually username) is stored on the block.

3. The third information that every block in the blockchain contains is the information about itself. Just as anything/anyone else in this world, everything needs its own identity to be able to distinguish from others. Same is the case with the blockchain blocks. Being usually implemented using hash tables, each block in the blockchain has a unique code called "hash". Again, taking the movie booking example, if you ever book 2 tickets of the same movie, same show, all the information from the above two pieces is exactly the same in both the blocks. Then, this hash value only is used to differentiate between both the blocks (transactions). Each block stores information of a single transaction. The size of which depends on the type of transaction and the information required to be stored.

2. WORKING OF BLOCKCHAIN

Blockchain is a structure where various blocks of information are strung together. So, when a transaction occurs, its details are stored in a block and then that block is added to the blockchain.

The working of the blockchain technology is indicted by the diagram below:-

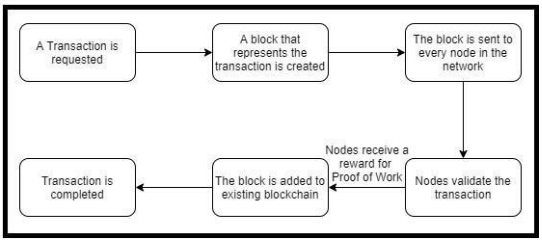

Fig. 1: Working of Blockchain technology

However it sounds easy, it consists of a total of four steps:

1. A transaction must occur – In order to add a block to blockchain, the block itself must be created. And since a block stores information about a transaction, at first the transaction must occur (done by user).

2. The transaction must be verified – After the transaction is done by the user, a network of computer works on its details (time, date, amount, digital signatures) in order to verify

whether it really happened in the way you said it did. And if yes, mark it as verified.

3. The transaction must be stored in a block – After the transaction is verified, now is the time to actually store its information in a block which later will be added to the blockchain. The information like time, day, date, amount, digital signatures of both sender and recipient are stored in the block.

4. The block must be given a hash number – As discussed earlier, hash is the unique code of a block to identify and distinguish it from other blocks in the blockchain. So, in order to add the block to the blockchain, it must be given a hash. Also, the block is given the hash of the last block added to the blockchain. Thus, every block contains two hashes in total, one of its own and one of the previous block.

Once the block is hashed, it can be added to the blockchain.

3. VISIBILITY OF A BLOCKCHAIN

There's no restrictions as such who can view the blockchain. Anyone can view it and also even connect to the blockchain network. When the user connects to the blockchain network, a copy of the complete blockchain is stored at the user's computer which is then updated every time a block is added to it. Since, there's a copy of blockchain stored at so many computers, to manipulate a data it should be updated at each and every computer. Which makes it difficult for the hackers to manipulate the data.

4. SECURITY ASPECTS OF BLOCKCHAIN

Blockchain plays a vital role in security concerns. Since every block in the blockchain contains its own hash and the hash of the previous block, if hash of the previous block is changed, hash of the current block must be updated too. These hash values of the blocks are generated by a mathematical model, which converts the other information like transaction and user details to some hash value. Therefore, if any information in the transaction is manipulated, the hash value of the block is changed. Let's consider if a hacker tries to manipulate a data of a

transaction (amount for example), the hash value of that block will change, but the next block in the blockchain still contains the previous hash value only. Thus, the updation will be marked invalid. So, the hacker will first have to calculate the new hash value (guess the right model used to generate the hash value) and then, update the new hash value in the next block, but which will then change the hash value of the new block. Similarly, if the hacker really wants to manipulate the data, he/she has do this process for the entire blockchain. Since, the height of blockchain is too large, it is way too difficult for the hacker to manipulate all the blocks. Thus, it is almost impossible to manipulate the data of a block once it's added to the blockchain.

Above problem also referred as trust issues, can be solved by a common technique called Proof of Work. In proof of work technique, the computer must prove itself that it has done 'work' by solving a complex computational mathematical problem. These computational problems are so difficult that the odds of solving any one of these problems is 1 in 5.8 trillion. This may not make the blockchain completely secure, but it does compel the hacker to solve such difficult computational problem that solving it would almost outweigh the benefits of the attack.

5. AN INSIGHT INTO APPLICATIONS OF INTERNET OF THINGS (IOT)

The Internet of Things (IoT) is a system of interconnected and interrelated devices like computing devices, mechanical devices which share data with each other over a network and work together to achieve a common goal.

With the evolution in IoT, nowadays it is mostly think of "Smart Home". But, smart home(s) is just one implementation of IoT, as it is also used in various other domains. Some of these domains are:

1. Military/Defense applications: In defense various sensors, cameras, signal radars, receivers are required to detect and monitor the activities at the borders, in the sky and at the security bases. In order to achieve this, all the sensors must send the data they acquire about the environment to the base stations.

2. Agriculture: One of the most innovative implementations of IoT can be seen in the field of agriculture. Using the sensors like humidity sensor, sensors able to calculate the amount of various minerals in the soil, and using the statistics and agricultural sciences, the data grabbed from the sensors can be used to tell the farmers about the crop health, necessities of minerals (if any) and various other details.

3. Weather monitoring: Though looks very basic, but it can be a real issue when it comes to monitoring the weathers of accident-prone areas (areas prone to landslides for instance). Many weather observers are dead as they had to be present at the site to do weather monitoring, but with the evolution of IoT, now sensors can be deployed to such areas which then send the weather information of the area to the news stations.

6. BLOCKCHAIN TECHNOLOGY AND IOT

Now that the importance and usage of both Blockchain and IoT are discussed. Let's see how they both are connected and more importantly, what the need of both to be together is.

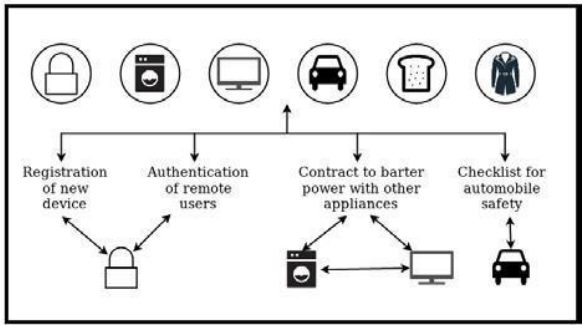

Fig. 2: Integration of Blockchain technology into IoT

Security and privacy have always been major concerns in the field of IoT which is mainly due to the massive and distributed nature of IoT networks. Vulnerability of IoT systems in security and privacy concerns can result in mass destruction of both economy and life (for instance, the sensors at the country borders are hacked and thus cannot detect the attack, can lead to a mass destruction). This is where blockchain comes into the picture. As already discussed about the security measures of blockchain, it can be integrated with IoT systems to make them secure. Although, it sounds very simple to integrate blockchain into IoT, but there are issues in it too. Since most of the IoT systems are real-time i.e. the information from the IoT devices must be transferred to the host over the network in real time (instantaneously) and blockchain implementation requires a huge number of calculations which adds the latency to the data transfer process which again is a great issue if considering the same previous example but also creates a need of high-end computing IoT systems.

So, the main requirement for implementing blockchain technology in IoT systems is reducing the latency.

7. RELATED WORKS

In [1], authors have focused on reducing the latency and the computing needs using cloud and fog platforms to host blockchain services. Cloud and fog both are almost similar to each other except, cloud having more of computational power which creates latency issues while fog on the other hand being less computationally powerful, has a lower level of latency as compared to cloud. In the proposed paper, the authors performed a simple experiment using Intel Edison Arduino boards as their IoT device which was connected to a Wi-Fi hotspot with three standard workstations that host python servers that interact each with a multichain node. The board executes ten concurrent clients that perform writes (720 bytes) to the multichain (via python server). The runs along with delays are also shown in the paper. Then, IBM's Bluemix blockchain technique is implemented to this system using both cloud and fog as the blockchain hosting platforms and the performance of both is analyzed. Based on the analysis results, it was concluded that network latency in the performed experiment was the dominant factor (as compared to computational resource availability). Thus, fog outperforms cloud.

In [2], the authors manage security issues related with IoT in a "miner" which is a highly developed device used for handling communications within a smart home using a protective, local and private Blockchain technology. To decrease the scalability, the resource consuming POW is eliminated and thus the use of inferred technology is made in the mentioned smart home system. The further overhead delay is reduced by using clusters in the overlays and placing a cluster head (CH) at the center of each cluster this also provides a distributed format in the smart home tier. The various components of the smart home includes: transactions, which intermediates between the overlay nodes and to secure the various transactions a shared key is used. Next component is Local Blockchain for each of the transactions. Another component is the Home miner which as the name suggests is used as a processor central to the smart home to manage the incoming and outgoing of various transactions. Besides various other functions the minor also appends the block to the blockchain after receiving all transactions. Last component of smart home is the local storage which helps in storing the data using FIFO method and can be unified with the miner or accessed separately. The steps involved in the smart home working are: Initialization, Transaction Handling and shared overlay. Initialization includes a genesis transaction i.e. adding a device to the blockchain using a shared key which lays within the genesis transaction. Next, Transaction handling which any internal or external interaction of the smart devices is seen through the owner using a shared key this ensures the security and also provides an invigilation over the communication between the devices. Lastly the shared overlay comes into play when the owner has two homes i.e. two miners in which case there is a central shared miner used. There can be sharing of the genesis transaction between each home. The overall evaluation of the security and performance of the smart home systems highlights: First, for security analysis, confidentiality and integrity were achieved in the three process of smart home working while availability can be archived using shared keys through which the devices communication is monitored by the miner. Further discussing the benefits the security attacks of Distributed denial of service attack (DDOS) and linking attack is blocked by the hierarchy of protection checked by the miner and the shared unique key usage respectively.

In [3], authors have proposed a new system architecture to implement blockchain in IoT systems. In this architecture, no IoT device is directly a part of the blockchain thus reducing the need of computing resources. Instead, the authors have defined a concept of smart contract which defines the access control rules of the system stored in blockchain and thus cannot be changed once put on the blockchain. The whole proposed architecture can be divided into two parts, one part being IoT system which includes IoT devices and the management hub and the other part being Blockchain network which includes miner, smart contract, agent node which is responsible for actually creating the smart node and deploying it on the blockchain. Once the smart contract is successfully put on the blockchain, the agent node has the smart contract's blockchain address which is useful to interact with the smart contract. In the implementation of the proposed architecture, the authors have used Ethereum as the blockchain technology and the

experiments were performed on Ubuntu machine using vertigo/ethereum image for the docker to implement the blockchain system. The experiment was conducted and compared for two scenarios, first one to evaluate the performance of management hub independently i.e. requests being made from virtual clients to the IoT device(s) in the setup and the second scenario being requests for resource information being made from one virtual IoT device to another IoT device. Both the scenarios were run for multiple concurrent clients for the sufficient amount of time and in both the scenarios, blockchain did grant all the requests to all the resources. The security analysis for both the scenarios was done using STRIDE model which is acronym for spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privileges. The blockchain part of the architecture did provide a great level of security but IoT devices not being the part of blockchain rely on the management hub for their access control decision and thus a malicious management hub can spoof the system. Apart from this single issue, the proposed architecture when compared with currently used architectures appeared to be more reliable, usable, heterogeneous and light-weighted.

In [4], the authors mentioned the significance of Blockchain in the Bitcoin technology which helps in the security, privacy and technical aspects with its vital distributed ledger. Although having its use in various projects other than Bitcoin the limitations such as its long block generation period of ten minutes limits its use and thus Ethereum with a short block period and a highly shared computing system for IOT devices comes into play. Talking about Ethereum, though it has a short block period of 12 seconds this makes the performance slower. Ethereum based systems becomes more stabilized and matures with time. Managing IOT devices using Ethereum can be observed using a scenario where a few hundreds of smart phones and a few Raspberry Pis acts as meter to measure the electricity usage. The processes are configured and connected through Ethereum which handles all the involved processes concurrently. The Ethereum model is rather different from the client- server model in terms that the Ethereum is present in each device making the transactions but the presence of BC maintains security and keeps the attackers at bay. The way of smart contract brought in Ethereum helps in using it as a computing platform and also helps in reducing the malicious attacks by simply ignoring them in lack of a valid account and public key. Meter contract in a smart contract is used to save the electricity use as the associated meter sends values to the blockchain in a repeated cycle which can be managed by the other entities, now this method requires a policy contract which helps the Ethereum account to access the policy and the public key registered in contract. In the conclusion to the experiment on the Ethereum it is concurred that although the Ethereum has a small transaction time it still proves to be lacking in some domains and including a proxy for the problem with the light client compromises the security of the system. Also the use of large storage to resolve the security compromise is still expensive and thus not reliable.

In [5], as the title of the paper suggests, the authors have implemented the blockchain in IoT in order to secure the user identity. The authors used permissioned blockchain to achieve this as it meets the fundamental requirements for longevity, agility, and incremental adoption. The key features that the authors have used to achieve the transaction longevity are:

- Asymmetric Key Rotation – This contains the existence of two keys – public and private which are useful to perform the sharing of an information oven an unreliable channel. The private key is unique and secret for each user while the public key is shared with the message useful to decrypt the shared (encrypted) information.

- Device Group Membership – There are two basic approaches when it comes to proper key management. First, being the key to be created on the used they are used for. Second, there shouldn't be a transaction of keys from one device to another. Thus, the keys are meant to be user specific and not device specific. This way all the devices belonging to a common user will have the same key and belong to the same group, so that even if any device moves out of the group, the user who did the transaction can be identified.

- Hash Function Agility – In this, hash function used by blockchain is used (say SHA2), using that the parallel hash values for the same transaction (say SHA3) are created and stored, so that even if the signature scheme used for past transactions becomes vulnerable, signing a different message as an attempted replacement will result in a different hash value under the parallel hash regime.

- Transaction Expiration – How long should the details the details of a transaction be stored? The answer to this question is different for the different areas of application of the system. But as IoT devices have a little storage with them, it may not be enough to store the required number of transactions. Thus, each old transaction is referred to by its next transaction just like done in git.

Using the above features and creating a transaction certificate for each authorized user only enables to hide the identities and other attributes like entitlements or even affiliations to be secured and can only be access and added by the users with a transaction certificate.

In [6], the resilience of the data in IoT using the blockchain technique is discussed using the scenario of a cloud based drone. With the increase in the use of internet in the embedded systems the devices able to connect and compute data through cloud computing increased significantly but this leads to increased cyber-attacks and modification of data thus to solve this problem the Blockchain method was used in IoT which helps in improving the security and privacy of the data using its shared key system, decentralized architecture and public key infrastructure. The model for the blockchain in IoT specifically follows the objectives: Firstly, trusted data origin then instant and permanent data integrity, trusted accountability and a resilient backend. Talking about the system architecture for the BC based Drone system or the DroneChain the main component includes the blockchain network along with drones and control system and a cloud server. The blockchain for the drone system helps in the data validation and resilience through its decentralized network. Since the cloud server has the data collected from the drones managed in a database which can

be vulnerable to security breach the DroneChain application helps to keep a check on the data this comes under the treat model. The key establishment is necessary to encrypt the necessary data and the keys used are called as a drone registration key, a data encryption key and a data access public/private key pair. The implementation of DroneChain consists of the collection and transmission of data done in seven steps in which the important entities are the drone registration i.e. the collection of the data as a node, data and command transmission, blockchain receipt generation where future validation and tracking is done after blockchain transaction next entity is cloud data validation and lastly the data auditing and decision making. The evaluation of the DroneChain system is based on two main aspects i.e. the security analysis stating the significance of BC for the secured and resilient drone communication which helps to preserve high level of data transfer, and performance analysis where the simulation made for collection and transmission of data shows the capability of the system for the collection of different sized data and the stabilization of the average response latency in the observed time range.

In [7], authors focus on discussing the importance of blockchain, IoT and importance of blockchain integration in IoT systems. Authors divide the integration of blockchain in IoT in 5 different possible scenarios:

- Gateway as a full blockchain node: The IoT devices/modules being the end node in the system can communicate with the IoT gateway which can then implement the full blockchain functionality i.e. securing the transaction.

- Gateway as a thin client: The gateway in this scenario only stores the relevant information of the transaction, thus working as a thin client.

- End-devices as regular sensors: If the end devices are battery powered sensors, they may not be so powerful as to integrate a blockchain client to them. Thus, IoT gateway pushes the data to the blockchain infrastructure.

- End-devices as server-trusting client: A simple form of blockchain client utilizing an interface like BCCAPI may be integrated to battery powered end-devices.

- End-devices as thin client: If end-devices are not battery-powered and always-on, they can operate as a thin client.

If blockchain based IoT systems can be implemented worldwide, it will make various processes like application development, data processing and other works to be done with these smart systems only as then, they will be secure too.

In [8], the author mentioned the use of coordinated satellite terrestrial networks to improve the efficiency of the blockchain technology used in IoT. The communication in blockchain is entirely peer to peer based where each node shares an equal status. There is a satellite present to broadcast the transactions involved and the blocks present in the blockchain which helps to improve the propagation speed. In a blockchain system, for a successful transaction is it necessary to be broadcast to maximum number of nodes which in case of P2P transmission depends on the blocksize and the number of neighbors that each node can connect denoted by K. Increasing the block size increases the transactions and the TPS but sometimes has a negative effect. It was concluded by Kiayias and Panagiotakos that blocksize is not a useful factor to affect the TPS, while on the other hand increasing K decreases the total propagation delay which helps in improving the TPS. Due to the broadcast feature and the coordination with the terrestrial networks the satellite system is beneficial for the blockchains and this can be studied from their use in the CSTNs. The performance evaluation of the CSTN using the satellites for blockchain concludes, as the increase in the nodes in the terrestrial network the TPS decreases. In a small network the TPS of the CSTN is approximately same as the terrestrial network but in order to outperform it, the CSTN needs to have a big network size.

In [9], authors use a concept called ‘smart contract’ along with ‘Hyper-Ledger Fabric’ proposed by IBM team in Blockchain infrastructure to make the IoT communication secure. Let’s first dive into what a smart contract is. This is a computer program which is used to transfer and monitor the assets or digital currencies among parties under certain rules. In blockchain, these smart contracts are stored in the blocks only which provides even more security to the infrastructure due to the immutability and security of the blockchain itself. Using hyper-ledger fabric overcome some limitations present in the permissioned blockchain like performance overhead and confidentiality. The mechanisms which are being used currently in the IoT systems is centralized which may be useful in current IoT industry but can’t cope up with the rapid growth of the IoT industry. Thus the authors suggest a decentralized mechanism which will also remove the issue of peer-to-peer communications between IoT nodes, also reducing the cost of installation and maintenance. Since the proposed mechanism is decentralized, the storage and computational load is also distributed all over the system. And as discussed earlier, for the security concerns, smart contracts and hyper-ledger fabric is implemented. Authors have also shared the performance and security analysis of the proposed mechanism and compared with that of already existing ones.

In [10], author discusses the introduction of a new behavior monitor to be used as a trust confidence to outside networks in the Blockchain based IoT setup. Also, for the secure execution environment for the applications a Trusted Execution Technology is incorporated. The function of TEE (Trusted execution environment) can be seen in Intel’s Software Guard Extension (SGX). The threat model considers the TEE as trusted from the beginning and assumes the communication between the IoT devices and the behavior monitor as secure. In the proposed model, all the communications must pass through the blockchain for validation. For the behavior monitor the process of the detection of the behavior and its monitoring comprises of four steps i.e. data collection, feature extraction, training model and continuous monitoring. The evaluation of the proposed architecture is made using a smart home setup where the behavior monitor is made the main node for each of the present zone. For this, Intel SGX was used as a rootof-

trust for security of the blockchain and the results proved its capability in the mentioned task.

In [11], authors have given a clear picture of not only why to implement blockchain in IoT systems but also how is it done. The authors explain about how IoT being decentralized and heterogeneous in nature is already providing security at a small scale. But using blockchain, which is the backbone of bitcoin (the first crypto-currency introduced in 2008) this small scaled security of IoT systems can be enhanced and they can then be used in wider applications and almost everywhere, as the lack of security is the only reason of many fields not accepting the IoT solutions. The authors then introduce a new type of blockchain that is specifically optimized for IoT. Authors have explained their proposed solution for smart home only, but the same can be implemented in various other fields too. The proposed framework mainly consists of three tiers: smart home, overlay network, and cloud storage. The end IoT devices use a private Immutable Ledger which works similar to blockchain but is centralized. Higher resource devices jointly create a distributed overlay that instantiates public blockchain. But the blocks are appended to the blockchain without doing the proof of work which decreases the computational load on devices and also the delay in the IoT transactions. A distributed trust method is employed in the overlay to decrease the computation in validating a new block. Thus using this architecture, the authors were able reduce both the computational and storage delays in the IoT systems.

In [12], the author mentioned the use of IoT and Blockchain in a smart district i.e. a city equipped with rapid development of services, integrated grids in buildings and homes which is also capable of saving energy. The main concern is given on building an integrated network for the communication between hardware and software using sensors. The proposed model is in the area of Bergamo, Italy. It is modeled for both the inhabitants and the collective management of a controlled center located in the residential area. The KNX interface was used as the main protocol. The energy consumption was reduced by using methods such as timer setting of the appliances, using photovoltaic system overload monitoring etc. Security is also a major task of the home automation which is achieved by installing video surveillance with motion detection connect with the devices such as phones for the user. Other security systems are perimeter alarm clock with fingerprints etc. There are several measures for the protection in case of lightning etc. The various automation system can be controlled using a single monitor such as switch, phone software etc. Another use of IoT is the Innovation Park consisting of various features such as smart playground with cameras, automatic slides, smart relax, smart parking, info point with a smart card, smart swimming pool, electric bike sharing, car sharing etc each of whose functionality and use is discussed in the paper. The use of Blockchain is beneficial as it not only helps consume less energy but also helps to produce energy with a high degree of autonomy. One example is the use of solar panels. However, due to the interoperability of different household devices the implementation smart home is still difficult.

In [13], authors have proposed a new energy framework based on deep learning and blockchain and named it as Deep Coin. For low/medium voltage distribution, blockchain based architecture in used in smart grid. In this framework, the nodes connected to the smart grid network are able to sell their extra energy to other nearby nodes (e.g. HAN) or to some distance (e.g. BAN and NAN). Multi-signatures and anonymous messaging streams for decentralized energy trading networks is implemented for privacy preservation of the trading information. In the blockchain of energy entities such as energy nodes, energy aggregators and smart meters are used which in combine is very effective for doublespending attacks. Another scheme for data aggregation and privacy preservation is by having multiple groups with each group having a private blockchain. For provenance and transparency in the smart grid system, Grid Monitoring framework which use smart contracts between the companies and the user by adopting cryptographic primitives such as consumer private key, consumer public key, and authentication contract key. For protection against malicious attacks on the metering infrastructure, Intrusion detection system (ISD) such as HANIDPS is implemented using ZigBee is installed at the BAN and NAN nodes and is responsible for verification of the frames running in energy transaction comply with the set of rules. HANIDPS is effective against IEEE 802.15.4 attacks such as replay attacks, denial of service against guaranteed time slot (GST), radio jamming etc. Next is the payment which is done by DeepCoin inspired from Bitcoin structure.

In [14], the author focused on the use of blockchain and machine learning in healthcare sector. In this first the patient will be certified from the authority then the patient will be able to access his/her details but will not be able to access details of any other person. To perform this every verified user will have a shared ledger by which he/she will be able to access his/her data. The real data can be acquired from health check-ups, surveys, interviews, fitness devices such heart rate, blood pressure etc. It then will be fed to a machine learning models which can help in detection and prediction of diseases such as diabetes, cancer, heart problem etc. It can be affected by the quality and quantity of data fed, if both the factors are satisfied, the efficiency will be more. The suggestions provided to the patient will also be fed into models on the basis of which the patient will be getting advices on lifestyle. If the raised any issue regarding his/her health, the model on the basis of symptoms and previous training with the help of Natural Language Processing will be able to identify the disease and also capable of providing treatment suggestion. Along with the patient information, healthcare sector also has a lot of machines and equipment which themselves have their own life span. The blockchain network will also give suggestion regarding when to change or remove the machine.

In [15], the author focused on various applications of machine learning where block chain can be used. Supply chain is associate integrate method of converting raw material into finished goods by multiple business personal such as makers, suppliers, distributors which creates huge amount of data and is stored in databases in clouds. But by dividing the information then storing it in multiple servers will increase the security which machine learning is capable

of build such models and by applying blockchain technology will make the structure more secure. A digital form of terms and conditions is Smart contract which can be easily created by someone who handles dataset by using blockChain technology which will be helpful to monetize the skill of the individuals who are good in machine learning algorithms which then can be upgraded to Artificial Intelligence by using better advance learning models. BlockChain provides shared and confined along with tracking of resources responsibly. By combination of Artificially Intelligent chatbots and blockChain can create a trusted and secured mechanism to get those benefits. In healthcare, blockChain chips can be implemented to achieve accuracy medication in insurance industry. The deep knowledge about patient such as qualities, family ancestry and way of life can help in much more accurate prescription and quality treatment. In this field, Artificially Intelligent analyzing can keep precise historical information of patient by using cryptographical records. One good implementation of Off-BlockChain communication is by making the vehicles communicate with the help of IoT devices. The vehicles get to know about the availability and on that basis comparison for better takes place such as nearby gas station, parking and suitable selection will be done on the basis of cost and other factors.

8. SURVEY ANALYSIS

Table 1. Summary of Survey Analysis

After the designing phase, there comes the implementation part. The following application was implemented in JAVA with MYSQL in the backend. A database was created to store the login/register user and to store the places with user ratings.

REFERENCE NUMBER	PUBLICATION SOURCE AND YEAR	MAJOR CONTRIBUTION	AREA OF APPLICATION
[1]	IEEE, 2018	Addressing latency issues in cloud Addressing computational issues in fog	Cloud and Fog platform
[2]	IEEE, 2019	Resolving the security issues in IoT Decreasing the Scalability	Smart home systems
[3]	IEEE, 2019	Proposing new system architecture for blockchain Reduction in computing resources	IoT Systems
[4]	IEEE, 2018	Security, privacy and technical aspects	Bitcoin and Ethereum Platform
[5]	IEEE, 2019	Increasing the transaction longevity	Securing user identity
[6]	IEEE, 2019	Resilience of data in IoT	Cloud based drones and embedded systems
[7]	IEEE, 2019	Blockchain integration with IoT	Smart Systems
[8]	IEEE, 2019	Improving the efficiency in communication	Satellite terrestrial networks
[9]	IEEE, 2019	Secure communication in IoT	IoT devices
[10]	IEEE, 2018	Establishing trust confidence to outside networks.	Communication between IoT and external devices
[11]	IEEE, 2018	Small scaled security	Smart home solutions
[12]	IEEE, 2018	Integrated network for communication between hardware and software systems Reduction in energy consumption Security issues	Smart city solutions
[13]	IEEE, 2019	New energy framework based on blockchain and deep learning Privacy Preservation	Smart grid networks
[14]	IEEE, 2019	Privacy Preservation Detection and prediction of diseases	Healthcare sector
[15]	IEEE, 2019	Addressing the security concerns Cost optimization	Supply chain management

9 CONCLUSION

IoT has become an integral part of everyday human life. It has wide spread applications in the areas of healthcare, communication, agriculture, smart city solutions, smart home solutions, supply chain management, networking to name a few among many others. The major concern in IoT is security and privacy preservation. This major concern is addressed in the recent times using blockchain framework and methodology. The survey conducted also reveals the same. Irrespective of the area of application, the blockchain technology has been able to address the various problems effectively providing optimal solutions. The blockchain technology has furthered enabled progress in this field of IoT and its application by addressing the various concerns.

REFERENCES

1. Wang, T., 2018, December. *"A unified analytical framework for trustable machine learning and automation running with blockchain"* in 2018 IEEE International Conference on Big Data (Big Data) (pp. 49744983). IEEE.
2. Lu, Y., Tang, Q. and Wang, G., 2018, November. "On enabling machine learning tasks atop public blockchains: A crowdsourcing approach" In 2018 IEEE International Conference on Data Mining Workshops (ICDMW) (pp. 81- 88). IEEE.
3. Tanwar, S., Bhatia, Q., Patel, P., Kumari, A., Singh, P.K. and Hong, W.C., 2019. "Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward" in IEEE Access, 8, pp.474-488.
4. Dey, S., 2018, September. "Securing majority-attack in blockchain using machine learning and algorithmic game theory: A proof of work" in 2018 10th computer science and electronic engineering (CEEC) (pp. 7-10). IEEE.
5. Shrivastava, V. and Kumar, S., 2019, February. "Utilizing Block Chain Technology in Various Application Areas of Machine Learning" in 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon) (pp. 167-171). IEEE
6. Kim, H., Kim, S.H., Hwang, J.Y. and Seo, C., 2019. "Efficient privacy preserving machine learning for blockchain network" in IEEE Access, 7, pp.136481-136495.
7. Bravo-Marquez, F., Reeves, S. and Ugarte, M., 2019, April. "Proof-ofLearning: a Blockchain Consensus Mechanism based on Machine Learning Competitions" In 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON) (pp. 119- 124). IEEE.
8. Shen, M., Tang, X., Zhu, L., Du, X. and Guizani, M., 2019. "Privacy preserving support vector machine training over blockchain-based encrypted IoT data in smart cities" IEEE Internet of Things Journal, 6(5), pp.7702-7712.
9. Tanwar, S., Bhatia, Q., Patel, P., Kumari, A., Singh, P.K. and Hong, W.C., 2019. "Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward" IEEE Access, 8, pp.474-488.
10. Dey, S., 2018, September. "Securing majority-attack in blockchain using machine learning and algorithmic game theory: A proof of work" In 2018 10th computer science and electronic engineering (CEEC) (pp. 7-10). IEEE.
11. Wang, T., 2018, December. "A unified analytical framework for trustable machine learning and automation running with blockchain" In 2018 IEEE International Conference on Big Data (Big Data) (pp. 49744983). IEEE.
12. Yogeshwaran, S., Kaur, M.J. and Maheshwari, P., 2019, April. "Project Based Learning: Predicting Bitcoin Prices using Deep Learning" In 2019 IEEE Global Engineering Education Conference (EDUCON) (pp. 14491454). IEEE.
13. Ferrag, M.A. and Maglaras, L., 2019. "DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids" IEEE Transactions on Engineering Management.
14. Vyas, S., Gupta, M. and Yadav, R., 2019, February. "Converging Blockchain and Machine Learning for Healthcare" In 2019 Amity International Conference on Artificial Intelligence (AICAI) (pp. 709-711). IEEE.
15. Shrivastava, V. and Kumar, S., 2019, February. "Utilizing Block Chain Technology in Various Application Areas of Machine Learning" In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon) (pp. 167-171). IEEE