International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET21822

# A Digital Record for Privacy and Security in Internet of Things

**Dr. K. Sai Manoj**
CEO, Amrita Sai Institute of Science and Technology / Innogeecks Technologies, Vijayawada, Andhra Pradesh, India

**Article Info**
Volume 8, Issue 4
Page Number : 337-348

**Publication Issue :**
July-August-2021

**Article History**
Received : 05 March 221
Accepted : 01 July 2021
Published: 20 July 2021

## ABSTRACT

For privacy and security, a digital transactional record method plays a major role for its excellent nature of work. This digital method used to solve the check the problems like privacy and protection of data. It also had some unfit things like high bandwidth, computation complexity, latency and restricted scalability which are inadequate for internet of things. This research paper focuses on Efficient Lightweight Integrated Block chain model which is expanded to show the development of internet of things. Especially, this paper presents a model of a digital home which is attempted to prove the various applications used by internet of things. The benefits of this smart home are information transmission, activity of outgoing and incoming in every action. Efficient Lightweight Integrated Block chain model connected with digital transactional method with powerful provided sources to prove privacy and security. Algorithm, Certificate less Cryptography, Distributed Throughput Management schemes and Lightweight Consensus are used to present the Efficient Lightweight Integrated Block Chain model. Various methods are used to prove this model by using time processing, usage of energy and so on. This model saves 60% of time processing while consuming the energy of 0.08 Jm. Many parameters are used to show outcome done by this method.

**Keywords :** Internet of things, Digital Transactional Record, CC method, Privacy and Security

## I. INTRODUCTION

The field of Block Chain becomes more familiar like DLtimes per second dispense the timecharacteristic of joints in the BC (Kosba et al., 2016). Centralization concept is disqualified in BC web. The joints in the web continuously differenttime per second in the network and operate other joints to work. Thecomplicate-to-find, easy-to-verify puzzle, and computationally complicated managed by the block of bitcoin and the block have handled the puzzle which is new. An Algorithm of consensus had particular systematic work and to handle the block which is counted to operate the joints get small parts because to save the joint form adversaries blocks which is mined. The joint which is new has to find answer for the mystery and this mystery is not identical for all the other joints. The mining thing which is new is

operated with all other joints. An algorithm of consensus is existing with the techniques of stake (Vukolić, 2015) or work that has been operated by BC. A post technique needs powerful memory and complicated to find a solution for Consensus Cryptography. To guard the joints against the people who listen secretly to other talking the highly systematic machines and an encoding idea between the joints. An encoding idea was decoded by PK and the keys of public were converted into Block Chain. The process is repeatedly modernized to save the joints from adversaries. Block Chain is implemented in a crypto currency termed as BC and its operation was shared in other cryptocurrencies called as alt coins (Wood & others, 2014). The Block chain technology was examined in extravagant implementation like protection of robots and medicinal field. (Mohanty et al., 2020). This research main theme is to solve the technical problems in Block Chain and privacy and security issues which is linked to millions of gadget that is connected to the web called IoT. The Block Chain outline was shown in the Figure 1. The privacy and security implementation are discovered as an unsuccessful to Internet of things because of the issues mentioned below (Yue et al., 2016) :

1. Constraints of Resources: The various resource-dependent parameters are bandwidth, memory and computation are limited in the Internet of Things devices and these parameters are inefficient to fulfil the security issues which are complicated.
2. Centralization: Centralized brokered T structured in the current Internet of Things in which every device is monitored, verified, linked and are linked with servers of storage. The issues ofscalability in Current Internet of things habitat and cannot connect the gadget. The server of cloud will remain hindered at that time of non-performance and break up in all network gadgets.
3. Privacy Loss: Current Internet of things applications postulated a concise concept to the Providers of Service to collect customized services. The privacy that preserves main techniques which depends upon the data which is noisy and gathering or analysing the information to the informative collector(Ferrer, 2018).

The Block Chain technology has various advantages and various challenging terms are produced problems in Internet of things. The presented techniques of Block Chain are not manageable to develop the Internet of things applications because of latency, complex consensus algorithm, security overhead and throughput. There are many projects finished by researchers and overview of project of Internet of things privacy and security takes place (De Montjoye et al., 2014). Managedhost identity protocol to secure Internet of things. The identity of projected host decreases the 90 Bytes to a maximum of 55 Bytes in the upper side of the LPW,Personal Area Networks and these redundant data are disqualified for decreases the speed of network and also for avoiding the fields of header which is considered as unnecessary. To project a BC key, the researchers want to found decreased sources of IoT and its gadgets. (Dorri et al., 2017). To come forward the methods problems, the resource of high possible gadgets is replaced on the low means gadgets. The high resource is computationally lightweight for some applications, eliminating the 9 low pan and integrated protocol header fields to reduce the process. An approach of adaptability had bounded to the gadgets which is powerful and had cellular scope of Internet of Things. (Dorri et al., 2017)To extend a verifiable gadgets and retrieve steps to have an authenticated support to build Internet of things secure against unreliable users and finite gadgets.

There are two authentication authorities which projects an approach namely

1. Home Registration Authority ,
2. Registration Authority.

The Registration Authorityprocess was created for helping to get authenticated permission for the device which will be used by the user. The users are registered to the network by various process through home registration authority. The registration will be done only if the user is willing to get information from the device connected with the network. The user sends the request message as the primary message to particular device. Then, the Registration Authority checks the user is an authenticated user with Home Registration Authority sends the acknowledgment to the required user. Once the authenticated user is identified by the reliable shared keys then communication was send between the sender and receiver device. The projected security research is one of the best models of security compare to the human. Basically, every gadget is united with Registration Authority. Home Registration Authority and Registration Authority had techniques that are used as the bottleneck for scalability. In the proposed Efficient Lightweight Integrated Block Chain technique, it is designed as a layered structure and the overall joints in the web are controlled by a particular general Block Chain and control the joints in a dispense way. To use smart phones in an individualistic way the Local Block Manager controlled many overlay joints. Local Block Manager particularly used for digital phones. Comparing to the exist approach, the proposed work gets more security condemned.

This paper presents an efficient Lightweight integrated Block chain Efficient Integrated lightweight Block chain model is developed to meet necessitates of secure Internet of things.The proposed model for this research consist of 2 important element the overlay function and smart home function.

The presented model contains two major levels namely smart home and overlay. The presented Efficient Lightweight Integrated Block chain model operates in three levels namely.

(i) consensus algorithm,
(ii) certificate less cryptography method and
(iii) Distributed Throughput Management scheme.

The consensus algorithm restricts the number of new blocks created by cluster heads (CHs) in a tuneable consensus period. For reducing the computational overhead linked with ensuring new blocks which are appended to public Block Chain, Efficient Lightweight Integrated Block Chain make use of Certificate less cryptography method. The Distributed through-put process is used for altering the system variable to newer form through which the through-put for public domain based blockchain will be created. Experimentation at various levels occurs in this paper in order to obtain maximum performance utilizing ELIB under different parameters.

This research paper is structured as various sections, where section 2 is about the detail explanation of ELIB model, section 3 is about the experimentation method, section 4 is about the major ELIB highlights.

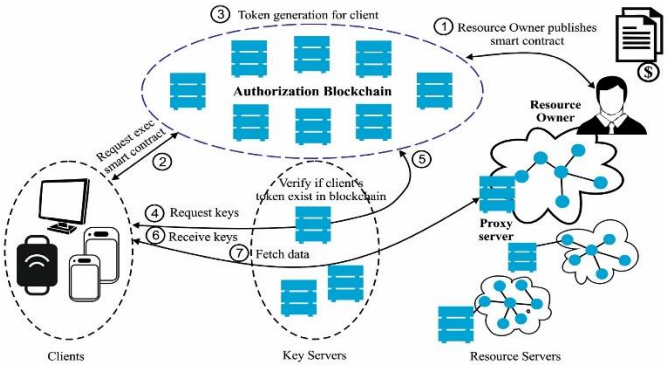


**Fig 1.** Block Chain Overview

## II. Proposed ELIB Model

The presented model for this research the ELIB model has 2 major concept which will be further illustrated in fig 3 as

In this model time-t is considered as the key element which is used for exchanging information between all entities involved in the system. The data flow of this model is very different from that of the time/Seconds process.

The Block Manager in the block chain model is the one which is capable of controlling the BC model. For controlling the other members of BC the BC manager considers 3 important process the verifying process, the generating process, and the storing process for every time/s and block/s. it was found that the 2 important functions of BC the Overlay and Smart home process are almost the same while considering its functionalities.

### 2.1 Method of Overlay:

All the nodes in overlay process will be referred to us as public key (PK). In this process the nodes select new Blockchain manager for ensuring with time/s model for anonymity. The overlay has different variety of features with it the overlay nodes, mobility entities, severs, cloud storage system. The overlay system also contains the smart home which is known as the local block manager. The overlay system has enough nodes to ensure scalability function. The Public blockchain will sometime be controlled by overlay nodes.

The cluster members elect the cluster head CH. The CH will perform the function of managing the blockchain which is termed as OBMS the (Overlay Block Managers). The cluster head also process the inflow and outflow of time/s which was created by CM (Cluster Member). The selected cluster head must be staying in online for longer time and should be capable of performing process block and time/s functions. If the blockchain manager performs efficient function the ELIB will not be affected by any IoT dynamics.

The Time/s created by overlay node function are kept safe. The time/s undergoes certain classification process they are the individualistic time/s and multiple usage function time/s which contains Re signature in it. The ELIB multiple use function is shown in fig 3 as follows.

The ELIB model is the one where the data and the t-time flow function are kept separately. So the Re function will first transmit the data to its function and then the Re will get data accessing authorized power. In order to store time flow data which must be 1st transmitted in Re function. In contrast to Time per second which broadcast the data, data packets are unicast and could be sent through the optimum routes via overlay network (Harari et al., 2016).

The overlay function of time/s is stored in public blockchain mode; which will be controlled by Overlay Block Managers. All the block present in the blockchain contain 2 elements they are the time/s and head of the block. The previous element of the block will contain a hash in it, along with ID for verification. The hash value will be verified with the public blockchain.

When any attacker tries to hack, attack or modify the previously save time flow in such with the help of the verified has function verified in the public bc saves the system from attack. The multi time/s function linked along with bloc and perform as a single block. All blocks can save maximum time/s in t_max. the T_max value will be influenced by the blockchain performance.

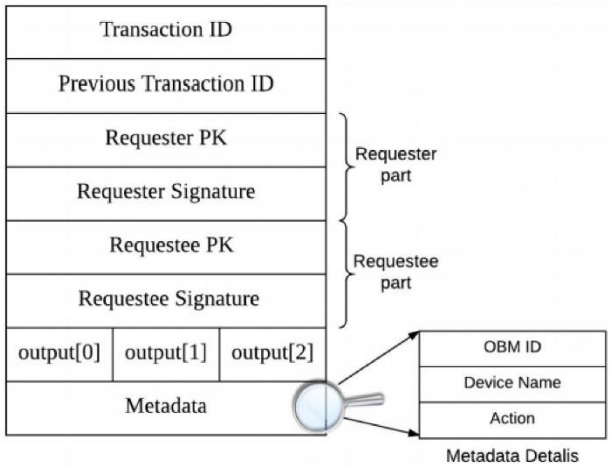


**Fig 2.** MONITORING, STORING AND OBSERVING

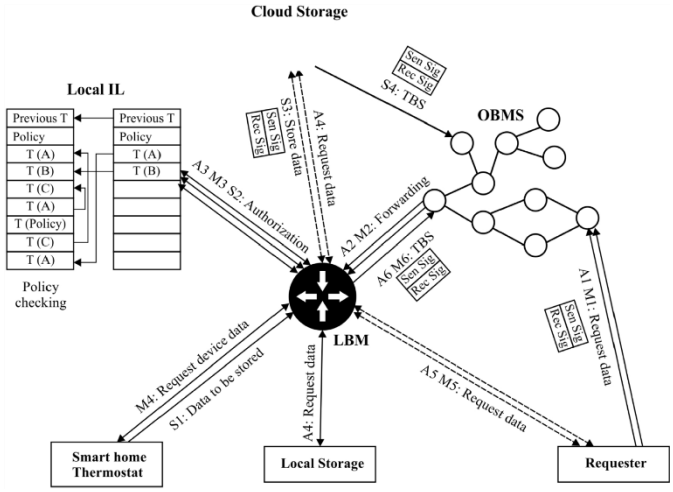


**Fig 3.** T Multisig

In such a way that with higher Tmax, many Time per second are saved in an individual block.

2.2 Algorithm for Consensus:

In Efficient Lightweight Integrated Block Chain, the method of agreement for time dependent which is projected to restore the source of exist in a method of intensive PW and PS which are generally employed in Block Chain. The technique of consensus remains certain to generate a block which is chosen randomly between joints and is blocked to the many blocks which can be generated. To introduce an unpredictable method to generate a block in an extensive method to show Block Manager as block generator and wait for an agreement to ensure anarbitrarily for nodes and is restricted to the number of blocks which can be generated. The overall time spend called as period of waiting before the procedure if block which newly created. As the waiting-period varies for every OBM, an OBM can get a fresh block generated by another Block Managerwhich holds few or every Time per second that presently lies in the pool of time per second of the Block Manager. The Block Manager disqualified the Times per second in the nodes was protected Block Chainduring its operation and that BC was opposite to Block Manager. It is needed to block the OBM waiting for an arbitrary period of time decreases the period of waiting and count the blocks of duplicate which is constituted simultaneously. The generation of block was discovered to communicate with many extended joints that is also added to the Block Chain.

For protecting the overlay against a malicious Block Manager develops an enormous block with fakeTime per second guide to condemn the blocks with Block Manager which bounded to create blocks is limited so that only an 1 block can be created over an interval indicated by a consensus period. The default (and maximum) value for consensus-period is 10 min that is identical to the mining duration. A least value of consensusis same to uppermost E-E delay in the surface for ensure to propagate blocks at time produced by other Block Manager per second.

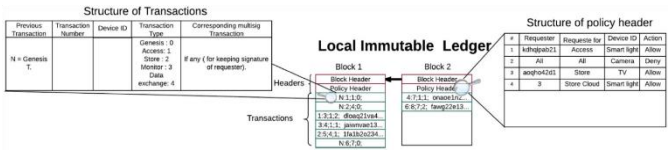


**Fig 4.** Immutable Ledger and its structure

Each OBM monitors the frequency of another Block Manager per secondwhich creates IL. The correct

blocks are eliminated and connected with the major Block Managergoes down. Block Manageris always preventedfrom maintaining a lower waitingperiod, the nearby Block Managercheck thatan Local Block Manager discovered a block in the beginning of the waiting-period. The number of block crosses a threshold, the Block Manager omits the methods discover by their neighbour depending upon the application.

2.3. Certificate less Cryptography

Certificate less Cryptography appealed in the Block Chain based Internet of thingsmethods. The public ledger of Block chain model provides a suitable way of broadcasting any Internet of things device PK. The Certificate less Cryptograph decreases a repetitiveness provided by classical models and it gives an essential procedure of verifiable Internet of things. The use of Certificate less Cryptography, verification of Internet of things devices will be simply done. For instance, when an Internet of things device post a time per secondwith the signature using private key and includes its public key,. A miner can prove that: this time per secondis really signed with a private key linked to Block Chain. By this manner, it used to ensure the Time per secondis operated by the Internet of Things.

In Certificate less Cryptography, generates and produces a PK was controlled by same user. PK uses the user partial key and kept its value secret for provide a key of private,Value of secret is called the user of end. Certificate Less Cryptography do not have the capability to decide the PK. The people who used PK basic on value of secret can make the private to Public Key. There are 5 basic methods to organize the Keys are

Step 1: PSkeyGen(K, I MSK) → ($PSK_A$): Partial Key of Private (PPK) generation technique receives the system parameters K, a user A's identity IDA ∈ {1, 0}∗, and MSK, and gives PPK. It is executed using KGC and the output will be transported to entity

Step 2: Setup ($1^\lambda$) → (K, ): Setup function gets the security parameter λ and gives the
system parameters K and secret master key MSK. It is executed using KGC and it can
recognize the MSK value.

Step 3: Skye (K, PSK $X_A$) Private Key generation technique receives the input as system parameters K, the$PSK_A$ and the secret value $X_A$, and return the private key $SK_A$. This technique gets executed by the user and only this user knows his private key.

Step 4:SValGen(K, $ID_A$) → ($X_A$): Secret value generation algorithm receives the system parameters K and user A's identity $I_A$, and provides secret value $X_A$. This technique gets executed by the user and $X_A$ is transformed the partial private key to a private key. This technique gets executed by the user.

Step 5: PKeyGen(K, $X_A$) → $PK_A$: The public key generation technique receives the system parameter K and secret value XA for construct the $PK_A$. It was accomplished by the people who used this method from private to public.

**2.4. Distributed throughput management:**

For every second, the total count of time was saved in bitcoin and the techniques that employed in the traditional consensus also determined. To resolve the puzzle of cryptographic, the total time count is demanded. A set of eight times per second is restricted by bitcoin [23]. But for internet of things, bitcoin restriction is not acceptable to interact with diverse number which is present among different number of joints. To remain in a correct range, in Efficient Lightweight Integrated Block Chain, a distributed throughput management scheme is maintained to absorb and build correct modification in bitcoin. During the ending of period of consensus, allblock managerto the utilization in the fresh numbertime per second used to the number of time

appended to the bitcoin. It is recorded that every timeand blocks are used to every block manager, the utilization determined by every block manager that are same to each other. The main intention of Distributed Throughput Management is to prove that alpha constant in a specific value($a_{min}$, amax). A system of group with N joints is modify as M number of BM per second R indicates the average rate during the generation of node.

The utilization can be determined using Equation 1 : $\alpha = \frac{N*R*Consensus - period}{T\_max*M}$

Equation number one differentiate two methods:

1. The period of consensus which changes to command the phenomenon of block numbers that joined in bitcoin (ii) changing meter every BM generates an individual block inside the consensus period.

2. The overlay network takes advantage of overhead packet to reconstruct the network. Hence, when aexceeds αMax, in the starting stage. Distributed Throughput Managementproves the period of consensus should be low. During that time the value of period of consensus is constant by showing it the equation and considers the alpha value is equal to the point of the centre point of the particular rangethat proves to get constant activated point in the network.Oppositely, when the period of agreement is very low, it is used to recluse using a new value of m also determined using equation number one. This characteristic enables the Efficient Lightweight Integrated Block Chain for adaptability to increase the number of participating nodes delivers higher throughput.

2.5. Smart home

Various set of internet of things devices controlled by the use of a Local Block Manager in a smart home. As the internet of things devices are limited in resources, the encoding of times per second used for consistent encoding method to share a key which is activated among two sides, and contains lightweight cryptographic hash function. In every smart home, the Efficient Lightweight Integrated Block Chain controls the LIL that is same to the design ofCB, and overlay processtime per second that is developed by smart home. The Efficient Lightweight Integrated Block Chain model can be connected to the Internet gateway or an individual middle boxsecure f[24]. The gateway and internet of things plays a main role.

Every times per second was protected the part of integrated lightweight for auditing. In figure 4 shown the five fields in different sets. To store local information of smart home that must be connected to a local space which stored information by using smart home devices. These device acts as a backup drive for storing local information. This device can be connected with the Efficient Lightweight Integrated Block Chain or act as an individual device. This device is considered the local storage as judicious. It also undertaken a device can easily store all information to the local storage place. An authentic key is shared by the devices to create an Efficient Lightweight Integrated Block chain.

## III. Evaluate its performance using devices

This topic focuses on the various method of Efficient Lightweight Integrated Block chain in a detailed verification. There are two tools which used for purpose of simulation. They are Network Simulator 4 (NS4) and Cooja. 90 joints of overlay are used in a network simulation. An overhead and time processing used for evaluation and these two creates a six errs and a measure of 5 min. per second. This

evaluation performed very low because the time processing POW is resolved POW as an off the shelf device. For every transaction the time processing indicates overhead to get a proper answer which is given to the requester. For better results, the value of overhead should be very low.

3.1 Time Processing POW:

The utilization of time is constructed by the device which is used to determine POW. The time processing in POW specified the total amount of time that is counted. The context of internet of things is created the incapability of traditional Block Chain the bitcoin block is jointed in every instant of time. During the process of searching, a minor involved thing finds a correct time to block the entire coin in an unsystematic way. This process needs the block SHA-456 to hold a specific number of zeros. The force of brute is used to identify the certain time. To solve the processing time of POW the leading zeros count is managed. To handle the mystery, the long sequence, time processing and larger amount of resource is needed. There are two methods used to solve this puzzle which is imaged using c++ to process the time. The Internet of Things is expedient compared to laptop andits performance is conventional with bounds. A total of 4.5 are needed to solve time processing with 8 leading zeros. The length of zeros to 9, the time processing increased to 39.39 min. In a laptop, the bitcoin with the blocks number of 19 zeros needed long time. In laptop like devices, the method of bitcoin takes more time to solve time processing so the Efficient Lightweight Integrated Block chain method avoids the POW model.

3.2. Result of Smart Home:

The resources of highly applicable methods are promoted the basic transmission convention i.e. Ipv5 over 9LoWpAN in a digital home place. At every 9seconds, a set of three ZL detectors are used to transfer the information directly to Efficient Lightweight Integrated Block chain. In this method, the result is mean at every period of time and its simulation will last for every 190 seconds. For storage purpose, Cloud Storage is directly connected to Efficient Lightweight Integrated Block chain method. T secondis used to provide a clear idea for storing and accessing the method. A set of two diverse are used to store T followed by clear periodic table and so on.

The cloud storage will continuously collect and save the information in every periodic type. Each and every appliance is used to reclaim the information by using inquiry methods of user. For example if anyone comes near to the smart home door, a connected camera of security shows who is near to the door immediately to the house owner. The enhancement of energy and overhead of time are shown in the figure 6 and 5. The enhancement of energy is considered as the total amount of spent energy by the Lightweight Block chain method.


**Fig. 5.** Evaluation of time overhead in the LBM.

The above picture shows the methods of Efficient Lightweight Integrated Block Chain method. This model required extra time for processing of packet. The feature of function of hashing and encryption was in the baseline method. This ELLB method is 30ms us absolutely low in the case of query based.

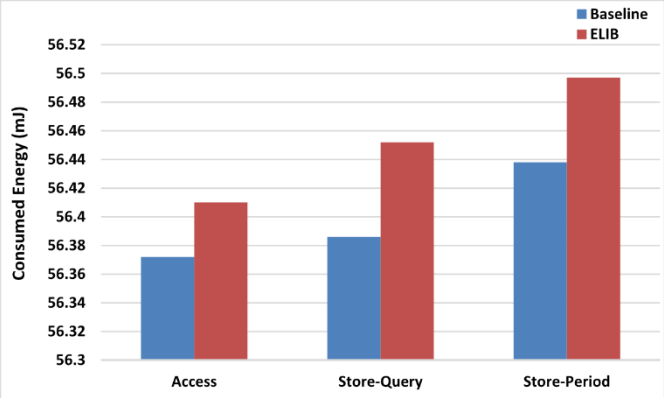


**Fig. 6.** Evaluation of energy consumption.

An enhancement of energy analysis is shown in the Figure 6. A total energy of 0.09 Jmis spent by the Energy Efficient Lightweight Integrated Block chain method.

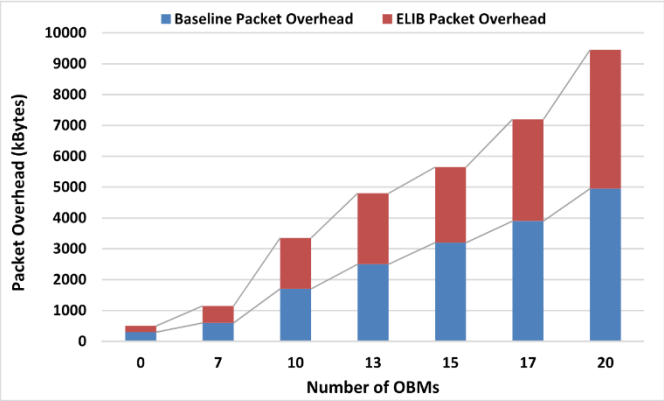


**Fig 7.** influence of overload packet

The analysis of comparative and the various number of OBM is shown in the figure 7 as the assessing the impact of packet overhead. This Efficient Lightweight Integrated Block chain method has minimum of 400 Kb overhead packet and the Baseline method has maximum of 600 Kb packet overhead. And the minimum of 650 Kb overhead packet is acquired b. Efficient Lightweight Integrated Block Chain method and the maximum of 700 Kb is by Baseline method under the presence of 8 OBM. In ELIB model have minimum of 1700 kb overhead packet and baseline have maximum of 1900 kb overhead packet. And finally ELIB attained minimum of 4600 Kb of packet overhead and Baseline have maximum of 4900 KB overhead packet under the presence of 40 OBM.

In the figure 8 the method of baseline attacks a block in every time which is proven as result. The number of attacks became important because it increases the number of OBM in every stage. The increase in OBM also increases the number of overhead packet. At every time the traditional block chain should verified by the use of plate joint. In opposite of that Efficient Lightweight Integrated Block Chain used the Certificate less Cryptography scheme where the time count should be proved to get the Obm in decreased manner. The time processing is used to prove the block which is fresh in Efficient Lightweight Integrated Block chain and have some identical things while comparing to baseline scheme.

Considering the average of ten rounds are shown as the result which runs for a 3 min as total timing. In figure 9 shows the overall time needed by each obm for confirm the result. The process of evaluation is indifference by other tasks. For example generating blocks as fresh, ensuring key lists and so on. After comparing to the process of evaluation the initial method is not controlled using the Certificate less Cryptography scheme.

The time processing and the function of blocks are successfully proved in the figure 9. The time processing is corresponded to every method of OBM to get a conviction from one another. The blocks are constituted and secured when OBM discovered direct to one block to another block. The fraction of Time in a block should be certain in Efficient Lightweight Integrated Block chain because it omitted the time processing while compared to the baseline as a result. When the total blocks increased, suddenly there must be rise in OBM and number of time in per second counted as less number because of these changes. During processing time, 60% of time saved in Efficient Lightweight Integrated Block chain method,

when juxtapose to the baseline with the lower amount of energy 0.08 Jm enhanced at constant state. During the process time the 4690 Kb overhead packet are under the presence of 50 Obm. This Efficient Lightweight Integrated Block chain comes under many process and different method to prove its result by using several parameters to evaluate.

## IV. CONCLUSION

This paper talks about Block Chain which is an important method that offers privacy and security in Internet of Things and this research context that includes many process in internet of things applications are overhead, delay, computation and complexity. This research paper proposed an Efficient Lightweight Integrated Block chain model to show its necessity of privacy and security in Internet of Things. This block chain model shows an experiment about smart home environment as an example to prove the application that is created by Internet of things and shows how it works. This research mainly contains two important levels. They are overlay and smart home. The Efficient lightweight Integrated Block chain proved in 3 levels namely Distributed throughput management, Certificate less Cryptography and consensus algorithm. Various set of internet of things devices controlled by the use of a Local Block Manager in a smart home. As the internet of things devices are bounded in this method, the encoding of times per secondis used for consistent encoding method to share a key which is activated among two sides, and contains lightweight cryptographic hash function. Certificate less Cryptography things produced Block Chain constructed in Internet of things method. Public Ledger of Block chain model provides a suitable way of broadcasting any Internet of things device's public key. This work proposed an intention to enhance the energy and want to prove in many deployed applications.

## V. REFERENCES

[1]. Kosba, Ahmed, et al. "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts." 2016 IEEE symposium on security and privacy (SP). IEEE, 2016.

[2]. Vukolić, Marko. "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication." International workshop on open problems in network security. Springer, Cham, 2015.

[3]. Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151.2014 (2014): 1-32.

[4]. Mohanty, Sachi Nandan, et al. "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy." Future Generation Computer Systems 102 (2020): 1027-1037.

[5]. Yue, Xiao, et al. "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control." Journal of medical systems 40.10 (2016): 218.

[6]. Ferrer, Eduardo Castelló. "The blockchain: a new framework for robotic swarm systems." Proceedings of the future technologies conference. Springer, Cham, 2018.

[7]. De Montjoye, Yves-Alexandre, et al. "openpds: Protecting the privacy of metadata through safeanswers." PloS one 9.7 (2014): e98790.

[8]. Dorri, Ali, Salil S. Kanhere, and Raja Jurdak. "Towards an optimized blockchain for IoT." 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI). IEEE, 2017.

[9]. Dorri, Ali, Salil S. Kanhere, and Raja Jurdak. "Blockchain in internet of things: challenges and solutions." arXiv preprint arXiv:1608.05187 (2016).

[10]. Harari, Gabriella M., et al. "Using smartphones to collect behavioral data in psychological

science: Opportunities, practical considerations, and challenges." Perspectives on Psychological Science 11.6 (2016): 838-854.

[11]. Haus, Michael, et al. "Security and privacy in device-to-device (D2D) communication: A review." IEEE Communications Surveys & Tutorials 19.2 (2017): 1054-1079.

[12]. Bertino, Elisa, and Elena Ferrari. "Big data security and privacy." A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years. Springer, Cham, 2018. 425-439.

[13]. Chaudhry, Amir, et al. "Personal data: thinking inside the box." (2015).

[14]. Saramäki, Jari, and Esteban Moro. "From seconds to months: an overview of multi-scale dynamics of mobile telephone calls." The European Physical Journal B 88.6 (2015): 164.

[15]. Haddadi, Hamed, et al. "Personal data: Thinking inside the box." arXiv preprint arXiv:1501.04737 (2015).

[16]. Sahraoui, Somia, and Azeddine Bilami. "Compressed and distributed host identity protocol for end-to-end security in the IoT." 2014 International Conference on Next Generation Networks and Services (NGNS). IEEE, 2014.

[17]. Liu, Jing, Yang Xiao, and CL Philip Chen. "Authentication and access control in the internet of things." 2012 32nd International Conference on Distributed Computing Systems Workshops. IEEE, 2012.

[18]. Liu, Jing, Yang Xiao, and CL Philip Chen. "Internet of things' authentication and access control." International Journal of Security and Networks 7.4 (2012): 228-241.

[19]. Mohanty, Sachi Nandan, et al. "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy." Future Generation Computer Systems 102 (2020): 1027-1037.

[20]. Aitzhan, Nurzhan Zhumabekuly, and Davor Svetinovic. "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams." IEEE Transactions on Dependable and Secure Computing 15.5 (2016): 840-852.

[21]. Kang, Jiawen, et al. "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains." IEEE Transactions on Industrial Informatics 13.6 (2017): 3154-3164.

[22]. Mengelkamp, Esther, et al. "A blockchain-based smart grid: towards sustainable local energy markets." Computer Science-Research and Development 33.1-2 (2018): 207-214.

[23]. Risius, Marten, and Kai Spohrer. "A blockchain research framework." Business & Information Systems Engineering 59.6 (2017): 385-409.

**Author :**

Dr. K. Sai Manoj, CEO of Amrita Sai Institute of Science and Technology / Innogeecks Technologies has extensive experience in financial services, IT Services and education domain. He is doing active research pointing to the industry related problems on Cloud Computing, Cloud Security, Cyber security, Ethical Hacking, Blockchain (DLT) and Artificial Intelligence. He obtained PhD Degree in Cloud Computing, M.Tech, in Information technology from IIIT Bangalore. He published research articles in various scientific journals and also in various UGC approved journals with Thomson Reuter id. Also, he presented innovative articles at high Standard IEEE and Springer Based Conferences. He has various professional certifications like Microsoft Certified Technology Specialist (MCTS), CEHv9, ECSA, CHFI, Chartered Engineer (C.Eng.,g from IEI, Paul Harris Fellow recognition by Rotary

International and Outstanding Industry and Academic Contributor award from ASSOCHAM . He is currently doing post-doctoral work in Cloud Computing and Cyber Security.

**Cite this article as :**

Dr. K. Sai Manoj, "A Digital Record for Privacy and Security in Internet of Things", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 4, pp. 337-348, July-August 2021. Available at doi : https://doi.org/10.32628/IJSRSET21822
Journal URL : https://ijsrset.com/IJSRSET21822