PRESERVING CONFIDENTIALITY OF IOT USING BLOCK CHAIN APPROACH FOR SMART HOME

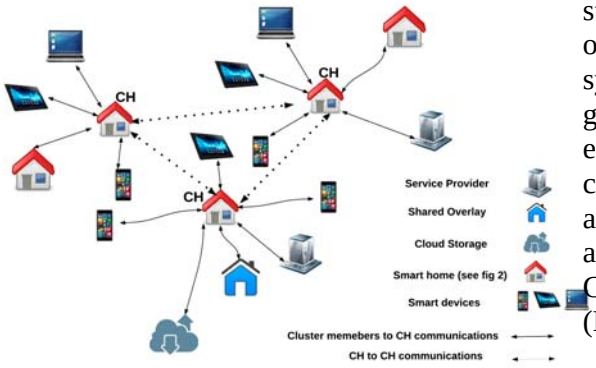
D. Anne Priya[1], S.Jananee[2], K. Malini[3]
[1,2]Assistant Professor, Dept. of Computer science and Engineering
C.A.H.C.E.T, Melvisharam, Vellore, Tamilnadu
[3]Assistant Professor, Dept. Of Information Tecchnology
C.A.H.C.E.T, Melvisharam, Vellore, Tamilnadu

Abstract
Internet of Things (IoT) security and protection remain a noteworthy problem, essentially because of the big scale and disseminated nature of IoT systems. Blockchain-based methodologies give decentralized security and protection, yet they include critical vitality, delay, and computational overhead that is not appropriate for most asset compelled IoT gadgets. Our approach was exemplified in a smart home setting and comprises of three fundamental levels to be specific: distributed storage, overlay, and keen home. In this paper we dive further and diagram the elements of the keen home level. Each equpped home is outfitted with a constantly on the web, high asset gadget, known as "minner" that is in charge of dealing with all correspondence inside and outer to the home. The minner likewise safeguards a private and secure BC, utilized for controlling and inspecting correspondences. We demonstrate that our proposed BC-based smart home structure is secure by completely investigating its security regarding the principal security objectives of privacy, honesty, and accessibility. At long last, we show illustration that overcomes the overheads (as far as movement, preparing time and vitality utilization) presented by our approach are immaterial in respect to its security and protection picks up.
Keywords: blockchain, security, IoT

I. INTRODUCTION

Internet of Things (IoT) comprises of gadgets that produce, process, and trade immense measures of security and safety critical information and also security touchy data, and consequently are engaging focuses of different digital assaults [1]. Some new networkable gadgets, which constitute the IoT, are low vitality furthermore, lightweight. These gadgets must commit the majority of their accessible vitality and calculation to executing center application usefulness, making the undertaking of moderately supporting security what's more, security very difficult. Conventional security strategies have a tendency to be costly for IoT as far as vitality utilization what's more, handling overhead. Also huge numbers of the condition of-theart security systems are very incorporated and are therefore not essentially appropriate for IoT because of the trouble of scale, many-to-one nature of the movement, and single purpose of disappointment [2]. To secure client protection, existing strategies regularly either uncover loud information or inadequate information, which may possibly impede some IoT applications from offering customized administrations [3]. Thus, IoT requests a lightweight, versatile, what's more, disseminated security and protection shield. The Blockchain (BC) innovation that supports Bitcoin the primary cyptocurrency framework [4], can possibly overcome previously mentioned challenges because of its disseminated, secure, and private nature. Bitcoin clients that are known by a variable Open Key (PK), produce and communicate exchanges to the system to exchange cash. These exchanges are pushed into a piece by clients. Once a square is full, the piece is attached to the BC by playing out a mining procedure. To mine a square, some particular

hubs known as mineworkers attempt to settle an asset expending cryptographic confound named Verification of Work (POW) [5], and the hub that understands the confound first mines the new square to the BC. In our past work [6], we contended that receiving BC with regards to IoT isn't direct and involves a few huge difficulties, for example, high asset request for understanding the POW, long inactivity for exchange affirmation, what's more, low adaptability that is a consequence of broadcasting exchanges what's more, pieces to the entire system. We proposed a novel instantiation of BC by dispensing with the idea of POW and the requirement for coins. Our proposed system depends on various leveled structure and dispersed trust to keep up the BC security what's more, security while making it more appropriate for the particular prerequisite of IoT. We exemplified our thoughts in the specific situation of a smart home, yet our system is



application freethinker what's more, can be connected in other IoT settings. The plan comprises of three center levels that are: smart home, distributed storage, and overlay. Smart gadgets are situated inside the brilliant home level what's more, are halfway overseen by a digger. Smart homes constitute an overlay arrange alongside Specialist organizations (SP), cloud stockpiles, and clients' cell phones or PCs as outlined in Figure 1. The overlay arrange is much the same as the peerto- peer organize in Bitcoin and brings the disseminated include to our design.

To diminish organize overhead and deferral, hubs in the overlay are gathered into groups and each bunch chooses a Group Head (CH). The overlay CHs keep up an open BC in conjunction with two key records. These key records are: requester key records that is the rundown of overlay clients' PKs that are permitted to get to information for the keen homes associated with this bunch; requestee key records that is the rundown of PKs of brilliant homes associated with this group are permitted to be gotten to. Distributed storage is utilized by the keen home gadgets to store and share information. We talked about subtle elements of the overlay and the cloud capacity in our past work [6].

This current paper's commitment is to give a complete dialog on the points of interest of the keen home level in our plan. We first blueprint how the IoT gadgets are initialised and afterward Clarify how exchanges are handled. A nearby and private BC is utilized for giving secure access control to the IoT gadgets and their information. Moreover, the BC creates a permanent time-requested history of exchanges that is linkable to other levels for giving particular administrations. The plan security comes from various highlights including: (1) in a roundabout way available gadgets; furthermore, (2) distinctive exchange structures in the shrewd home what's more, the overlay. To accomplish a lightweight security, symmetric encryption is utilized for smart home gadgets. We give subjective contentions to exhibit that the smart home level accomplishes classification, trustworthiness, and accessibility and furthermore talk about how key security assaults, for example, connecting assault [7] and Conveyed Disavowal of Administration (DDOS) are upset.

At long last, we exhibit quantitative outcomes utilizing recreations and demonstrate that the overheads incited by our system are generally little. Whatever remains of the paper is sorted out as take after: In Segment II we show the fundamental parts of the plan. The BC-based keen home is examined top to bottom in Segment III. Reenactment results and security exchanges are introduced in Area IV. Area V outlines related works, lastly Segment VI finishes up the paper.

II. CENTER PARTS

This segment examines the fundamental brilliant home segments as appeared in Figure 2. A. Exchanges Correspondences between neighborhood gadgets or overlay hubs are known as exchanges. There are distinctive exchanges in the BC-based smart home each intended for a particular capacity. Store exchange is produced by gadgets to store information. An get to exchange is produced by

a SP or the property holder to get to the distributed storage. A screen exchange is produced by the property holder or SPs to occasionally observing a gadget data. Adding another gadget to the smart home is finished by means of a beginning exchange and a gadget is evacuated by means of a evacuate exchange. The majority of the previously mentioned exchanges utilize a mutual key to secure the correspondence. Lightweight hashing [8] is utilized to distinguish any adjustment in exchanges' content amid transmission. All exchanges to or from the brilliant home are put away in a nearby private BlockChain (BC).

B. Nearby BC

In each brilliant home, there is a nearby private BC that keeps track of exchanges and has an approach header to uphold clients' approach for approaching and active exchanges. Beginning from the beginning exchange, every gadget's exchanges are fastened together as a changeless record in the BC. Each square in the nearby BC contains two headers that are square header and approach header as appeared at the highest point of Figure 2. The piece header has the hash of the past piece to keep the BC changeless. The approach header is utilized for approving gadgets and authorizing proprietor's control approach over his home. As appeared in the best right corner of Figure 2, the strategy header has four parameters. The "Requester" parameter alludes to the requester PK in the gotten overlay exchange. For nearby gadgets, this field is equivalent to the "Gadget ID" as appeared in the fourth line of the proposed strategy header in Figure 2.

The second section in the approach header, shows the asked for activity in the exchange, which can be: store to store information locally, store cloud to store information on the distributed storage, access to get to put away information of a gadget, and screen to get to continuous information of a specific gadget. The third segment in the arrangement header is the ID of a gadget inside the smart home, lastly, the last segment shows the activity that ought to be improved the situation the exchange that matches with the past properties. Other than the headers, each square contains various exchanges. For every exchange five parameters are put away in the neighborhood BC as appeared in the upper left corner of the Figure 2. The initial two parameters are utilized to chain exchanges of a similar gadget to each other and distinguish every exchange exceptionally in the BC.

The exchange's comparing gadget ID is embedded on the third field. "Exchange write" alludes to the sort of exchange that can be beginning, access, store, or screen exchanges. The exchange is put away on the fifth field on the off chance that it originates from the overlay arrange, something else, this documented is kept clear. The neighborhood BC is kept and overseen by a nearby mineworker.

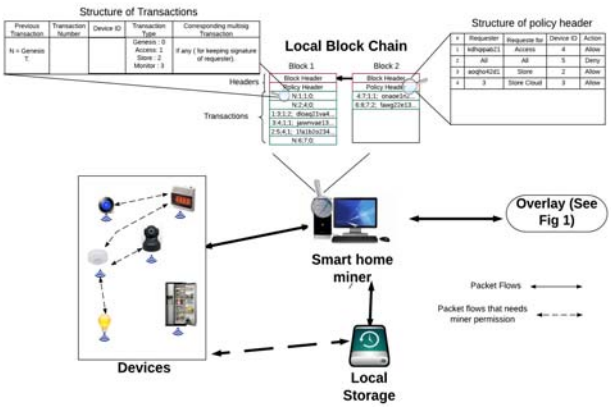


Figure 2 Smart home overview

C. Home mineworker

Keen home excavator is a gadget that halfway procedures approaching and active exchanges to and from the keen home. The mineworker could incorporate with the home's Web door or a different remain solitary gadget, e.g. F-secure [9], could be put between the gadgets and the home passage.Like existing focal security gadgets, the excavator verifies,approves, and reviews exchanges. What's more the excavator likewise achieves the accompanying extra capacities: creating beginning exchanges, dispersing and refreshing keys, changing the exchanges structure, and framing and overseeing the group. The mineworker gathers all exchanges into a square also, adds the full square to the BC. To give extra limit, the excavator deals with a neighborhood stockpiling.

D. Nearby Capacity

Neighborhood stockpiling is a putting away gadget e.g. reinforcement drive that is utilized by gadgets to store information locally. This stockpiling can be incorporated with the

mineworker or it can be a different gadget. The capacity utilizes a First-in-First-out (FIFO) strategy to store information and stores every gadget's information as a record anchored to the gadget's beginning stage.

III. THE BC-BASED SHREWD HOME

To begin with, we examine the introduction steps, exchanges dealing with, furthermore, shared overlay. A. Instatement In this area, we depict the way toward including gadgets furthermore, arrangement header to the nearby BC. To add a gadget to the shrewd home, the mineworker produces a beginning exchange by sharing a key with the gadget utilizing summed up Diffie-Hellman [10]. The shared key between the mineworker and the gadget is put away in the beginning exchange. With respect to characterizing approach header, the home structure in Figure 2 and adds the approach header to the to start with piece. The mineworker utilizes the approach header in the most recent piece in BC; consequently, to refresh the arrangement the proprietor should refresh the most recent square's approach header. proprietor creates its own strategies as per our proposed strategy

B. Transaction Handling

The keen gadgets may discuss specifically with each other or with substances outside to the shrewd home. Every gadget inside the home may ask for information from another inward gadget to offer certain administrations, e.g., the light demands information from the movement sensor to turn on the lights naturally when somebody enters the home. To accomplish client control over shrewd home exchanges, a mutual key ought to be assigned by the digger to gadgets which need to straightforwardly convey with each other. To allot the key, the mineworker checks the strategy header or requests consent from the proprietor and afterward disseminates a mutual key between gadgets. In the wake of accepting the key, gadgets convey straightforwardly as long as their key is substantial. To deny the give consent, the mineworker denotes the circulated key as invalid by sending a control message to gadgets. The advantages of this technique is twofold: on one hand, the digger(thus the proprietor) has a rundown of gadgets that offer information, and on the other, the correspondences between gadgets are secured with a common key. Putting away information on the neighbourhood stockpiling by gadgets is the other conceivable exchange stream inside the home. To store information locally, every gadget should be verified to the capacity that is done utilizing a mutual key. To give the key, the gadget needs to send a demand for the excavator and on the off chance that it has putting away authorization, the excavator produces a mutual key and sends the key for the gadget and the capacity. By accepting the key, the neighbourhood stockpiling creates a beginning stage that contains the mutual key. Having the common key, the gadget can store information straightforwardly in the neighbourhood capacity.

The gadgets may request to store information on the distributed storage that is known as store exchange. Putting away information in the cloud is a mysterious procedure that is talked about in [6]. To store information the requester needs a beginning stage that contains a piece number and a hash utilized for mysterious verification reason. The distributed storage might be either possessed and overseen by the SP (e.g. Home indoor regulator) or paid for and oversaw by the property holder (e.g. Dropbox). In the previous occurrence, the mineworker demands for the beginning stage by producing a marked exchange with the gadget key. In the last case, installment is done through Bitcoin. In either capacity write, subsequent to getting a ask for the capacity makes a beginning stage and sends it to the mineworker. At the point when a gadget needs to store information on the distributed storage, it sends information and the demand to the digger. By getting the ask for, the digger approves the gadget for putting away information on the distributed storage. On the off chance that the gadget has been approved, the mineworker removes the last square number and hash from the neighborhood BC, and makes a store exchange and sends it alongside the information to the capacity. Subsequent to putting away information, the distributed storage restores the new square number to the mineworker that is utilized for additionally putting away exchanges.

The other conceivable exchanges are access and screen exchanges. These exchanges are basically produced by either

the property holder to screen the home when he is outside or by SPs to process gadgets' information for customized administrations. By

accepting an entrance exchange from hubs in the overlay, the digger
checks whether the asked for information is on the nearby or the distributed storage. In the event that information is put away in the neighborhood stockpiling, the digger demands information from the nearby stockpiling and sends it to the requester. Then again, if the information is put away in the cloud, the digger either asks for information from the distributed storage furthermore, sends it to the requester, or sends the last piece number furthermore, hash to the requester. The last situation engages the requester to peruse whole information put away by the gadget in cloud capacity and is reasonable when the put away information are for a one of a kind gadget. Something else, the client's security may be imperiled as some portion of a connecting assault which is talked about later in Segment IV. By getting a screen exchange, the excavator sends current information of the asked for gadget to the requester. On the off chance that a requester is permitted to get information for a timeframe then the mineworker sends information occasionally until the point that the requester sends a nearby demand to the mineworker and abrogate the exchange. The screen exchange empowers property holders to watch cameras or other gadgets in which send occasional information. Keeping in mind the end goal to maintain a strategic distance from overhead or on the other hand conceivable assaults, the proprietor ought to characterize an edge in minutes for the intermittent information. On the off chance that the time in which the digger is sending information for the requester scopes to the limit, at that point the association is ended by the mineworker.

C. Shared overlay

At the point when an individual has in excess of one home, he needs isolate excavators and capacity for every one of the homes. To diminish the cost and overseeing overhead in this case, a common overlay is characterized. The mutual overlay comprises of at any rate two keen homes that are overseen midway as a solitary home by a mutual mineworker. The mutual overlay is like the keen home, notwithstanding, the structure of the mutual BC is distinctive to that of a shrewd home. In the mutual BC each home has a beginning exchange and the beginning exchange of all gadgets are affixed to their home's beginning exchange by the mutual overlay excavator. Another distinction in the common overlay is in regards to the correspondences between the homes with the mineworker. Gadgets that are in a similar home with the mineworker encounter no change, while for gadgets in different homes a Virtual Private System (VPN) association is set up between the Web door in each home and the digger of the mutual overlay that courses the bundles to the common excavator.

IV. ASSESSMENT AND INVESTIGATION

This area gives a total talk on the security, and execution of the BC-based smart home.

A. Security Investigation

There are three fundamental security necessities that need to be tended to by any security outline, to be specific: Secrecy, Honesty, and Accessibility, known as CIA [11]. Secrecy ensures that exclusive the approved client can read the message. Honesty ensures that the sent message is gotten at the goal with no change, and accessibility implies that each administration or information is accessible to the client when it is required. Utilized techniques to accomplish the initial two necessities are examined in Segment III. To build smart home accessibility gadgets are shielded from vindictive solicitations. This is accomplished by restricting the acknowledged exchanges to those elements with which every gadget has set up a mutual key.
Exchanges got from the overlay are approved by the digger before sending them on to the gadgets. Moreover, it can be contended that our BC-based structure just presents a minimal increment in the exchange preparing delays as contrasted with existing shrewd home entryway items. There is likewise an extra one-time delay amid instatement for creating what's more, circulated shared keys. In synopsis, the extra delays are not critical and don't affect the accessibility of the keen home gadgets.

Table I condenses how our structure accomplishes the previously mentioned security necessities

Next we break down the adequacy of our answer for counteract two basic security assaults that are especially applicable for shrewd homes. The first is Circulated Dissent of Administration (DDOS) assault in which the aggressor utilizes a few tainted IoT gadgets to

overpower a specific target hub. A few late assaults [12] have become exposed which have misused IoT gadgets to dispatch monstrous

DDOS assault: Our outline has a progressive protection against this assault. The main level of guard can be credited to the certainty that it would be outlandish for an aggressor to straightforwardly introduce malware on keen home gadgets since these gadgets are not specifically open. All exchanges must be checked by the mineworker. Give us for a minute a chance to expect that the assailant some way or another still figures out how to taint the gadgets. The second level of safeguard originates from the way that all cordial activity needs to be approved by the digger by looking at the strategy header. Since the solicitations that constitute the DDoS assault activity would not be approved, they would be obstructed from leaving the home. The following two protection layers are uncommonly composed and overseen by the objective of DDOS assault that can be any client in the overlay. These protection layers, that are conceding consent by utilizing CH key records and changing the PK in the CH key records, are talked about in our past paper [6] and are not in the degree of this paper. Connecting assault: To secure against this assault, every gadget's information is shared and put away by a special key. The excavator makes exceptional record of information in the distributed storage for every gadget utilizing an alternate PK. From the overlay perspective, the digger should utilize an exceptional key for every exchange.DDoS assaults.

The second is a connecting assault in which the assailant sets up a connection between different exchanges or information records with the same PK to discover store exchange we recreated two extraordinary and sensible movement stream designs:

B. Execution Evaluation

BC-based design brings about computational and parcel overhead on the shrewd home gadgets and the mineworker for giving enhanced security and protection. To assess these overheads, we recreated a savvy home situation in Cooja test system [13]. To look at the overhead of the BC-based design, we reenacted another situation that handles exchanges without encryption, hashing, and BC. We allude to this standard technique as the "base strategy". We utilized IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) as the basic correspondence convention in our recreation, since it is appropriate to the asset requirements for a keen home setting.We reenacted three z1 bit sensors (that mimick shrewd home gadgets) which send information specifically to the home excavator (additionally reenacted as a z1 bit) at regular intervals. Every reproduction gone on for 3 minutes and the outcomes introduced are found the middle lue of over this term. A distributed storage is specifically associated with the mineworker for putting away information and restoring the piece number. It is significant that the overlay postponement and handling is not considered in our reenactment. To give a complete assessment we recreated store and access transactions. For the store transaction we simulated two different and realistic traffic flow patterns:

Requirement	Employed Safeguard
Confidentiality	Achieved using symmetric encryption.
Integrity	Hashing is employed to achieve integrity.
Availability	Achieved by limiting acceptable transactions by devices and the miner.
User control	Achieved by logging transactions in local BC.
Authorization	Achieved by using a policy header and shared keys.

Packet Flow	Base (Bytes)	BC-based (Bytes)
From devices to the miner	5	16
From the miner to the cloud	5	36
From the cloud to the miner	5	16

- Occasional: In this setting, gadgets intermittently send their information to the distributed storage. This is genuinely run of the mill for different current smart home items, for example, Home indoor regulator.
- Question based: Thus, the gadget sends information on-request what's more, in light of a question got from the digger. This stream is proportionate to putting away information to the cloud by the home proprietor.

We assessed the accompanying measurements:

- Bundle overhead: Alludes to the length of transmitted bundles.
- Time overhead: Alludes to the handling time for each exchange in the excavator and is estimated from when a exchange is gotten in the excavator until the fitting reaction is sent to the requester.
- Vitality utilization: Alludes to the vitality devoured by the excavator for taking care of exchanges. The mineworker is the most elevated vitality devouring gadget in the keen home since it handles all exchanges and

performs bunches of hashing also, encryption. The vitality utilization of different gadgets is restricted to encryption for their own particular exchanges.

The talk on the assessment is as per the following:

Bundle overhead: Table II outlines the recreation comes about for parcel overhead. The table substance applies to both access what's more, store exchanges since both have a similar bundle measure. Utilizing encryption and hashing expands the parcels payload estimate; notwithstanding, considering the lower layer headers (i.e. 6Low- Skillet), the expansion in the information payload has generally little impact.

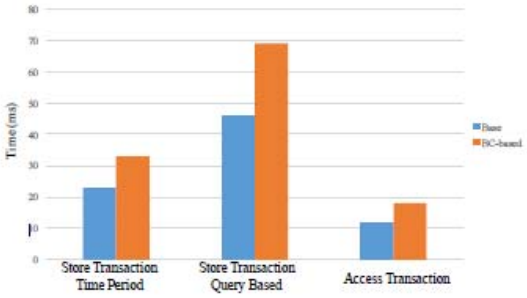


Fig. 3. Evaluation of time overhead.

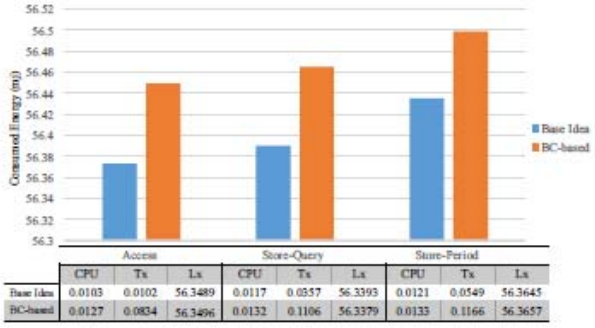
Time overhead: Figure 3 demonstrates the outcomes for the time overhead. The BC-based outline expends more opportunity to process bundles contrasted with the base strategy which can be credited to the extra encryption and hashing activities. In the most pessimistic scenario for the inquiry based store exchange the extra overhead presented by our technique is 20ms, which is still
little.

Vitality utilization: Figure 4 traces the vitality utilization comes about. As is obvious, the BC strategy builds the vitality utilization by 0.07 (mj). The table at the base of Figure 4 traces the vitality utilization for the 3 center assignments performed by the digger, in particular: CPU, transmission (Tx), and tuning in (Lx). The vitality utilization by CPU expanded about 0.002(mj) in our plan because of encryption and hashing. Transmitting longer information parcels multiplied the transmission vitality utilization of our technique in contrast with the base strategy. It ought to be noticed that we have accepted a 100% radio duty cycle in our evaluations (i.e. the radio is always on). radio is changed off irregularly to save vitality, at that point the relative listening overhead brought about by our strategy would be higher. In any case, notwithstanding accepting an extremely forceful obligation cycle of 1%, the relative increment in listening vitality would in any case as it were be around 60%.In synopsis, the low overheads presented by our BC-based technique essentially exceed given the huge security what's more, protection benefits on offer.

V. RELATED WORKS

There exist diverse examinations on security and protection of IoT what's more, savvy home. Creators in [14] exhibited that off-the shelf IoT gadgets need essential security shields by hacking into an assortment of shrewd home gadget including a light, switch and smoke caution. Creators in [15] contended that the shrewd homes are defenseless against assaults led by clients' cell phones regardless of whether the home door controls the trade of bundles to and from the home.

Creators in [3] proposed a strategy with three modules to secure clients' protection in the brilliant home. The information authority module gathers clients' information from the shrewd home and sends them to information recipient module that stores information in two unique datasets. The outcome module controls the client's entrance to information to ensure the security. This technique guarantees that lone the genuine client can get to information. In addition, by utilizing



	CPU	Tx	Lx	CPU	Tx	Lx	CPU	Tx	Lx
Base Idea	0.0103	0.0102	56.3489	0.0117	0.0357	56.3393	0.0121	0.0549	56.3645
BC-based	0.0127	0.0834	56.3496	0.0132	0.1106	56.3379	0.0133	0.1166	56.3657

Fig. 4. Evaluation of energy consumption in different traffic flows.

two datasets it is ensured that connecting distinctive information of a client to each other is outlandish.

In any case, the technique does not give security when the client requirements to uncover his information to a specialist organization.

VI. CONCLUSION

IoT security is picking up a considerable measure of consideration nowadays from both scholarly world and industry. Existing security arrangements are not really suited for IoT because of high vitality utilization what's more, handling overhead. We beforehand proposed a strategy that tends to these difficulties by utilizing the Bitcoin BC, which is an unchanging record of squares. The thought was talked about utilizing a savvy home as an agent contextual investigation. In this paper, we laid out the different center segments of the brilliant home level and talked about the different exchanges also, methods related with it. We likewise exhibited an comprehensive investigation with respect to its security and protection. Our reenactment comes about exhibit that the overheads caused by our technique are low and reasonable for low asset IoT gadgets. We contend that these overheads are justified regardless of their weight given the critical security and protection benefits on offer. To the best of our insight, this examination is the principal work that intends to improve BC with regards to shrewd homes. In our future research, we will explore the utilizations of our system to other IoT areas.

REFERENCES

[1] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in internet of things: The road ahead,” Computer Networks, vol. 76, pp. 146–164, 2015.

[2] Internet of Things – New security and privacy challenges

University Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.

[3] A. Chakravorty, T. Wlodarczyk, and C. Rong, “Privacy preserving data analytics for smart homes,” in Security and Privacy Workshops (SPW), 2013 IEEE. IEEE, 2013, pp. 23–27.

[4] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[5] S. King, “Primecoin: Cryptocurrency with prime number proof-ofwork,”July 7th, 2013.

[6] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in internet of things: Challenges and solutions,” arXiv preprint arXiv:1608.05187, 2016.

[7] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and cryptocurrency technologies. Princeton University Pres, 2016.

[8] A. Bogdanov, M. Kneˇzevi´c, G. Leander, D. Toz, K. Varıcı, and I. Verbauwhede,spongent: A Lightweight Hash Function. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 312–325.

[9] F.-S. sense, https://sense.f-secure.com/, [Online; accessed 19-November-2016].

[10] H. Delfs, H. Knebl, and H. Knebl, Introduction to cryptography.Springer, 2002, vol. 2.

[11] N. Komninos, E. Philippou, and A. Pitsillides, “Survey in smart grid andsmart home security: Issues, challenges and countermeasures,” IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1933–1954,2014.

[12] wired, https://www.wired.com /2016/ 10/internet-outage-ddos-dns-dyn/,[Online; accessed 10-December-2016].

[13]Cooja,http://anrg.usc.edu/contiki/index.php/ CoojaSimulator/, [Online;accessed 19-November-2016].

[14] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli,“An experimental study of security and privacy risks with emerging household appliances,” in communications and Network Security (CNS),2014 IEEE Conference on. IEEE, 2014, pp. 79–84.

[15] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, “Smart-phones attacking smart-homes,” in Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, 2016, pp. 195–200.