Secure Access Control to IoT Devices using Blockchain

PremanandGhadekar, NiketDoke, SushmitaKaneri, Varsha Jha

Abstract: ***Internet of Things (IoT) is growing at an exponential rate but the area of privacy and security in IoT still remains unexplored. The existing algorithms or methods are mainly centralized and hence they are vulnerable due to their single point authentication topology. As it has been estimated that by 2020 there will be more 'things' than people on this earth the problem of security becomes a major concern in IoT networks, as a person having control to an IoT network will be able to control a large portion of an organization. Blockchain has recently been used to provide security to peer-to-peer networks. Blockchains are computationally expensive, heavyweight and are considered unsuitable for IoT architecture. In this paper a new lightweight and secure architecture for IoT by using Ethereum Blockchain retaining most of its security providing powers is proposed. Since Blockchain is decentralized it solves the single point authentication problem existing in IoT networks. A Smart Home System as a representative case study has been implemented for broader IoT applications. The two parameters measured are temperature and intrusion detection. The proposed model tackles some more challenges that exist in IoT networks. The Qualitative evaluation of the proposed architecture highlights how it tackles various attacks.***

Index Terms: IoT, Access Control, Ethereum, Blockchain

I. INTRODUCTION

Internet of Things is unarguably the most disruptive technologies of the century. It is quite obvious that in the coming years the things that are not themselves computers will have some kind of computer inside them so that they can be connected to each other for communication and data exchanging purposes. It is quite easy to form an IoT network with the help of some cheap sensors and communication protocols and this data sharing will be at a higher granularity level but as the size and confidentiality level of the IoT network to be formed increases we can't ignore the security factor anymore. Sectors like smart city, smart healthcare, etc. can't afford to let the data of their organization be visible to anyone who wishes to view it since if one decides to misuse the data these organizations are generating then one will have posed a grave threat to these organizations financially as well as ethically..

On one hand, this data can be used to offer a range of personalized services to the users On the other hand, data contains information that can be used to reveal private behavior and lifestyle patterns.This shows the lack of fundamental security and privacy factors in the existing IoT architecture. A huge number of security and privacy vulnerabilities have already been identified in the existing IoT systems like smart locks, smart cars, etc.Several intrinsic features of a typical IoT architecture amplify the security and privacy challenges like: low storage and power capabilities, single point authentication, multiple attack surfaces, context-aware and situational nature of risks, and scale. In some papers people have tried to introduce distributed access control but they could not overcome the overheads and excessive delays that come with it. In many instances the benefit of IoT network and data sharing features cannot outweigh the risks of privacy and security. There is thus a need of security-aware sharing of data through IoT networks without compromising the privacy of the users. However, adopting Blockchain in IoT is not straightforward and will require addressing the following critical challenges: Mining is computationally expensive and time consuming and in IoT architecture low latency is expected which is difficult to provide using Blockchain. Blockchain scales poorly as we increase the number of nodes in the network and IoT networks contain a large number of nodes. IoT devices are bandwidth limited and certain miners may create a lot of traffic. The main aim of this paper is to introduce a Blockchain-based architecture for IoT devices and networks that delivers lightweight and decentralized security and privacy. The architecture retains the benefits of Blockchain while overcoming the challenges in integrating Blockchain with IoT. It helps to uniquely identify every node of IoT ecosystem with the help of Blockchain virtues of addressing.

II. LITERATURE SURVEY

A. Related Work

Ali Dorri, et. al in the paper [1] have proposed Blockchain-based IoT architecture handles most security and privacy threats, while considering the resource-constraints of many IoT devices. But the qualitative overhead analysis of the architecture has shown that it has constant performance overhead at best, and at worst most of its transactions scale with the number of clusters in the network, rather than considering number of nodes.

Revised Manuscript Received on 30 July 2019.
* Correspondence Author

PremanandGhadekar*, Associate Professor and Head of Information Technology Department.
NiketDoke, BTech in Information Technology from Vishwakarma Institute of Technology.
SushmitaKaneri, BTech in Information Technology from Vishwakarma Institute of Technology.
Varsha Jha, pursuing BTech in Information Technology from Vishwakarma Institute of Technology.

Steve Huckle, et.al have explored in [2], about how IoT and Blockchain technology can benefit shared economy applications. But there is no actual implementation of the proposed work. Also, it is not applicable to wearable IoT devices. Roman Beck, et.al in the paper [3] have given a proof of concept prototype that has the potential to replace a trust-based coffee shop payment solution. But, scalability issues, costs and volatility in the transaction currency are hindrance.Jose L.Hernandez-Ramos, et.al in the paper [4] have given access control solution support to the management of certificates, authentication, and authorization processes. Butsignature validation is a very expensive step which needs to be optimized. Delegation in the step of validation is also not done.

While, Ali Dorri, et.al have delveddeeper and outlined the various core components and functions of the smart home tier. Each smart home should have an always running, high computational resource device, known as ‘miner’ which will be responsible for handling all communication within and external to the home. But the overheads incurred due to the proposed method are very high and the method is specific only to Smart Home system [5].

Jesse Yli-Huumo, et.al in [6]. had the objective to understand challenges and future directions regarding Blockchain technology from the technical perspective. But the paper has excluded the economic, law, business, and regulation perspectives, and included only the technical perspective. Jing Liu, et.al mainly analyzed existing authentication and access control methods, and then, accordingly a feasible Internet of Things design is proposed. This paper doesn’t deal with DoS attacks [7].AafafOuaddah, et.al have proposed FairAccess as a new decentralized pseudonymous and privacy preserving authorization management framework that leverages the consistency of Blockchain technology to manage access control on behalf of constrained devices. There is no implementation of FairAccess and interfacing of IoT devices with Blockchain [8].Parikshit Mahalle, et.al presented the Identity Authentication and Capability based Access Control (IACAC) model with protocol evaluation and performance analysis. The method proposed is not a lightweight version of CAC for resource constrained devices in IoT like sensor nodes. Complete interoperability is an obstacle in this paper [9].

Rodrigo Roman, et.al have shown that the distributed approach has various challenges that need to be solved, but also various interesting properties and strengths. The main goal of this paper was to provide an explicit analysis of the features and security challenges of the distributed approach of the Internet of Things, in order to understand what is its place in the Future Internet. But there are numerous challenges that must be solved, such as ensuring interoperability, reaching a business model, and managing the authentication and authorization of entities which is not done in this paper [10].Jianjun Sun, et.al have proposed a conceptual framework with three dimensions: human, technology, and organization. They explore a set of fundamental factors that make a city smart from a sharing economy perspective. Space constraints and the population density of urban living are not considered in the proposed method [11].

B. Comparison of Blockchain Platforms

Blockchain Platform	Consensus Model	Transaction speed/sec
Ethereum	Proof of work (Proof of Stake 2018)	15 (1 million)
Hyperledger	Proof of Elapsed time	3500
Ripple	Byzantine Fault Tolerance	1500
IOTA	Directed Acyclic Graph	1000-2000
Neo	Delegated Byzantine Fault Tolerance	1000

Table 1. Blockchain Platform Statistics Comparison

PROPOSED MODEL

A. *Proposed Blockchain based IoT Architecture*

Consider a typical IoT scenario of a smart home where Alice has a number of smart devices like thermostat and intrusion detection device connected to cloud storage. The proposed architecture consists of 4-tier architecture consisting of end devices as the first followed by a gateway then private or public Blockchain and finally the cloud storage. This paper considers data access and data storage use cases. Alice should be able to access data about temperature remotely or smart device should be able to access each other based on access rights.

Moreover, these smart devices should be able to store data on cloud storage based on the access policies. Before discussing the details of architecture let’s introduce all the tiers.

1. End devices - This includes all the smart devices present in a smart home. As these devices don't have any unique identifier it is difficult to implement access control. Hence, proposed model introduced unique IDs which are addresses of account in the Blockchain. This address is in hexadecimal of length 40. Every address has a private key and hence only the ones with it can use this address for doing any transactions. Transactions are used for communication between devices.

So, every device has a unique address associated with it along with its device name. Whenever a device wants to send data to the cloud or talk with another device it has to use this unique address as a pass in order to carry out the task also known as a transaction. So, the address is needed to be kept safe inside the device and should not be shared with anyone.

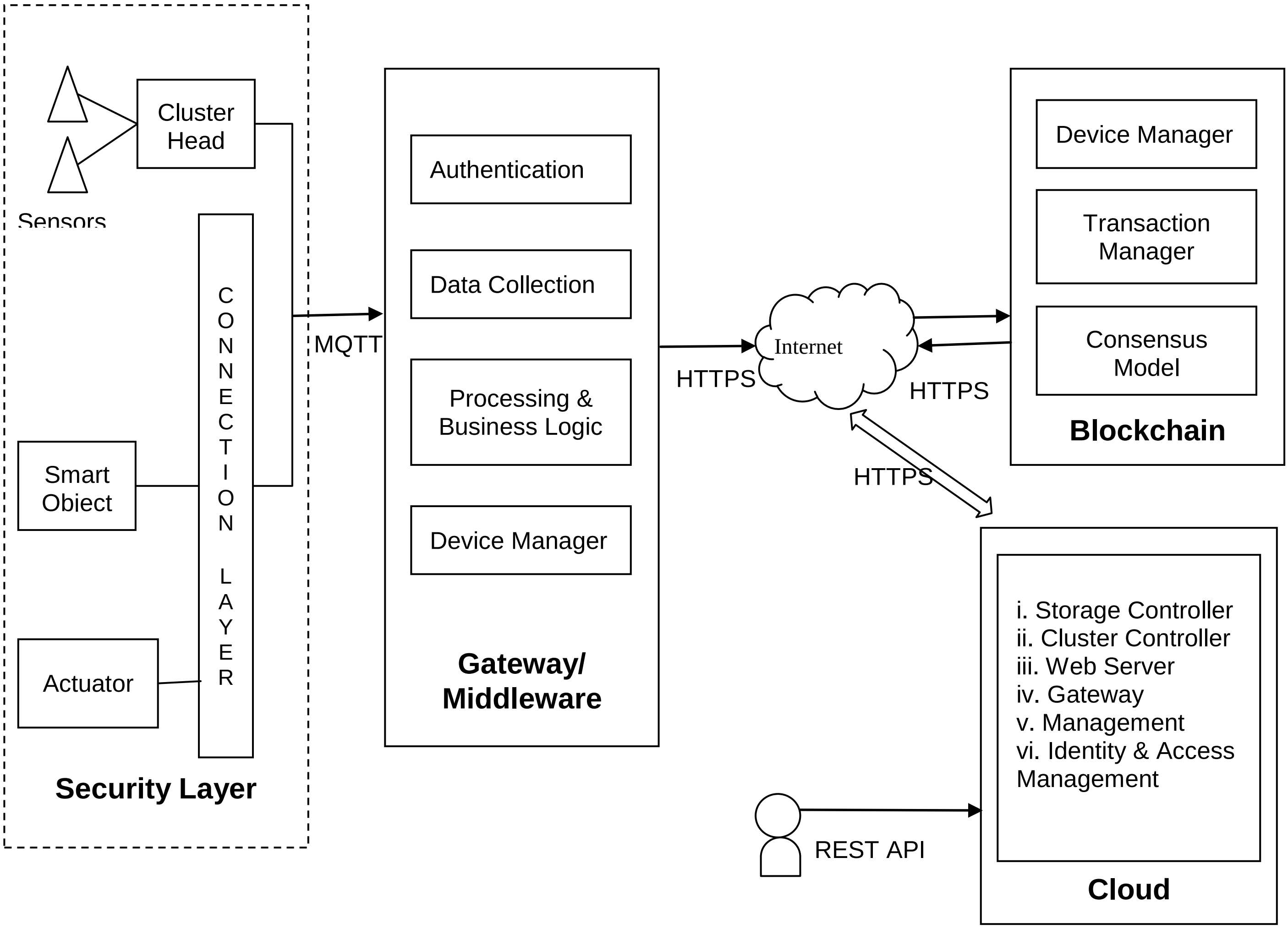

Fig. 1. Architecture of Proposed System for IoT - Blockchain

. Gateway - This acts as a mediator between the end devices and between the end devices and cloud storage by talking to a private or public Blockchain. This is also the place where the authentication of devices is done. The end devices and the local server talk with each other using MQTT (Message Queuing Telepathy Transfer), a lightweight protocol specially made for IoT devices. The device asks the server to store data to the cloud as it has access keys to do so. The local server also talks to Blockchain by calling a smart contract which has the logic to do all necessary logic. A smart contract is a computer code that runs on top of the Blockchain containing a set of rules under which parties agree to interact with each other. The smart contract stores the addresses of all the permissioned devices that are allowed to access other devices or cloud storage and grant access to them based on it. This part can be removed and the smart contract can be called directly by the end devices which is the part of the future scope.

3. Blockchain - This is the most important part of architecture which acts like an immutable database for authentication. Blockchain is peer to peer immutable database which helps in secure transactions. All the data is stored in the form of blocks in Blockchain which are connected to each other in the form of linked list referenced backwards. This Blockchain network can be a private or public depending on once choice. The local server talks with the Blockchain using http protocol. Here, a smart contract is been published on the Blockchain which helps in authentication. We have used Ethereum Blockchain and the contract is written in solidity language which is a JavaScript akin programming language. In Ethereum, you can set up a private Blockchain or use the public provided by them. We have used remix to deploy contract on ganache which is Blockchain emulator on localhost.

4. Cloud storage - This is storage used by smart devices to store the data collected by them continuously provided by a third-party provider. The cloud storage is only accessible from the local host. We have used Think speak for storing our temperature data on the cloud.

B. *Storing*

Each device may want to store its data on cloud storage based on its policies. For example, a smart thermostat typically stores data in the cloud storage to be used by the SP to implement certain smart services. Let's assume that Alice has created an account in a cloud storage facility and set up permissions for her thermostat to upload data to this facility. The gateway has access to cloud storage and hence any device that wants to store data on the cloud must interact with the gateway. Consider a scenario where thermostat has to store data on the cloud then it needs to send a token along with the data in encrypted form. The data is encrypted using AES algorithm to prevent man in the middle attack. The token is of form name:hash_code where hash_code is sha256 of unique_id given to that particulardevice concatenated by timestamp so that the hash_code changes every time transaction that is communication takes place between the devices. This token along with encrypted data is sent to the gateway. The gateway gets an encrypted list of permissioned devices by calling a smart contract on the Blockchain.

Later, each of this id is decrypted, concatenated by timestamp followed by a sha256 and then is checked with hash_code. If this hash_code matches it checks for other security policies and if everything is fine it sends data to the cloud.

C. *Accessing*

Communication between devices in IoT is very important and hence access should be provided in a secure way. Consider a situation where thermostat has to send data to another device and repeat this process. Gateway acts as an authentication device for this transaction. Thermostat will send a token of form source:destination:hash_code where hash_code is the same thing discussed above.

This token is attached to encrypted data which is sent to the gateway. The gateway gets an encrypted list of permissioned devices by calling a smart contract on the Blockchain. Later, each of this id is decrypted, concatenated by timestamp followed by a sha256 and then is checked with hash_code. If this hash_code matches it checks for other security policies and if everything is fine it sends data to the other device. Following is the flowchart for authentication.

Algorithm 1 Authentication and Access Control

```
hashtoken ← timestamp + deviceId
Append hashtoken to encrypted data
Send this hashtoken + data to the middleware gateway
whitelist ← Array of whitelisted deviceId from blockchain
i ← 0
flag ← False
whilei<len(whitelist) do
  ifSHA (decrypt(whitelist[i]+timestamp) == hashtokenthen
    flag ← True
    break
  end if
  i ← i+1
end while
if flag == Truethen
  Check access policies and send data to cloud
else
  reject the request and block the device if rejected thrice
end if
```

Contract Deployment Status:

STATUS	0x1 TRANSACTION MINED AND EXECUTION SUCCEED
TRANSACTION HASH	0xCF7B80AFFD04B2EE0485A7947E6C4E10C00256FFC3EE1CE4CFA3D83FD23316E8
CONTRACT ADDRESS	0x692A70D2E424A56D2C6C27AA97D1A86395877B3A
FROM	0xCA35B7D915458EF540ADE6068DFE2F44E8FA733C
TO	EDD.(CONSTRUCTOR)
GAS	3000000GAS
TRANSACTION COST	240030 GAS
EXECUTION COST	141390 GAS
HASH	0xCF7B80AFFD04B2EE0485A7947E6C4E10C00256FFC3EE1CE4CFA3D83FD23316E8
INPUT	0x608...70029
DECODED INPUT	{}
DECODED OUTPUT	-
LOGS	[]
VALUE	0WEI

Contract Invoked for adding members in whitelist:

status	0x1 Transaction mined and execution succeed
transaction hash	0x54f0f1357ac76ba60e0fe5277dac7505889dbe2d2da500800ed292b93194c825
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	edd.addMember(bytes32) 0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
gas	3000000 gas
transaction cost	48222 gas
execution cost	25542 gas

hash	0x54f0f1357ac76ba60e0fe5277dac7505889dbe2d2da500800ed292b93194c825
input	0x15b...00000

decoded input	{
	"bytes32 newAddress": "0xca35b7d915458ef540ade6068dfe2f44e8fa7333000000000000000000000000"
	}

decoded output	{}
logs	[]
value	0 wei

Contract Invoked for finding member in whitelist:

transaction hash	0xd17b8c14addae95582c760ba4ae39f1e1e1e1c9329d6f8fa54f9697c75ce6e02
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	edd.find(bytes32) 0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
transaction cost	26443 gas (Cost only applies when called by a contract)
execution cost	3763 gas (Cost only applies when called by a contract)
hash	0xd17b8c14addae95582c760ba4ae39f1e1e1e1c9329d6f8fa54f9697c75ce6e02
input	0xd43...00000

decoded output	{
	"0": "bool: true"
	}

logs	[]

Contract Invoked for fetching whitelist:

TRANSACTION HASH	0xb05ec4bc6d3fa4dad451c7d7edd3d849e529811d90f39f8dd125cf450019b57b
FROM	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
TO	edd.getElements() 0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
TRANSACTION COST	23207 gas (Cost only applies when called by a contract)
EXECUTION COST	1935 gas (Cost only applies when called by a contract)
HASH	0xb05ec4bc6d3fa4dad451c7d7edd3d849e529811d90f39f8dd125cf450019b57b
INPUT	0xb1a...18cc7
DECODED INPUT	{}

DECODED OUTPUT	{
	"0":"bytes32[]: 0xca35b7d915458ef540ade6068dfe2f44e8fa733a000000000000000000000000,0xca35b7d915458ef540ade6068dfe2f44e8fa733b000000000000000000000000,0xca35b7d915458ef540ade6068dfe2f44e8fa7332000000000000000000000000"
	}

LOGS	[]

EVALUATION

The main goal of evaluation is to verify the proposed model for attacks mentioned above and ensure access control.

I. Access Control: For any device to access resources on the network it must be authenticated and the authentication is done by checking with the whitelist on Blockchain. Hence, unless the device has a valid id present on the Blockchain, it can't access any resources. As the device id can't be only added by the admin which is quite secure the proposed model provides access control.

II. Man in the middle attack: For authentication the devices send SHA of current timestamp the authentication token are encrypted and the hash changes every time a device makes a request. For access control, man in the middle attack are possible if the attacker eavesdrops on the Id but as the token is hashed no one can extract device id from it.

III. Considering another man in the middle attack as replay attack, where some attacker intercepts the communication between the device and the gateway and uses the token sent by the device to gateway to listen to the conversation the timestamp would be invalid now and authentication will fail by verifying the timestamp T_u as it'll need time for sending the token after intercepting it. If T_u is older than the predefined threshold value, it is invalid and has been used.

IV. DoS attack: When the gateway receives the message from the end device, it checks the authentication token. If the token is invalid it discards the message. DoS happens when an attacker accesses particular resources massively and simultaneously. Controlling device using single id can be controlled by maintaining a single session. Moreover, if a particular device sends invalid token more than 3 times, it'll be blocked. Therefore, DoS attack can be prevented or at least minimized.

V. Unique Identification: Security can be provided if device is not able to be identified uniquely in the network. Market: Information breach can result into key concern of the entities like home, shop, company's data. Blockchain provides a unique account number to every node on the Blockchain network. This feature can be used to identify every device in IoT network which will act as either mining or passive nodes on the Blockchain.

VI. Data security: Most of the devices collect personal information along with other data and this data is not protected or encrypted. Companies which holds this data try selling it without consent of people and that's invasion of privacy. Data on rest should be encrypted. Also, data which is transferred must be encrypted and each user should have data visibility rights so that only trusted people can access their data.

VII. Centralizedauthentication: All authentication is centralized hence single point of failure if anyone hacks the server, he has access to devices.Decentralization and Blockchain has lot of market and buzz nowadays but again will people pay for this extra cost just for security and will manufacturer produce costly products Smart contract based authentication on Blockchain.

CONCLUSION

The network security is a pending challenge for the IoT industry which is quite trending. The proposed model in the paper uses Blockchain for providing secure access control to IoT devices. The proposed model exploits the immutability feature of Blockchain to store the whitelist of devices. The account number in Blockchain solves the problem of no unique identifier in IoT.

As the whitelist is stored on Blockchain, no one can alter its contents providing better authentication and access control. The timestamp and device id combination helps in combating man in the middle attack. The proposed model scales and is quite efficient for access control and uses combination of IoT and Blockchain.

FUTURE SCOPE

Current model was built using Ethereum Blockchain platform. The initial release which comprised of Proof of Work Consensus model was used. To scale up at better level we aim to implement the model using latest release of Ethereum which uses Proof of Stake providing more efficiency, reliability, trust, less time, less electricity consumption yet at faster speed rate.

- **Transaction Speed: 1 million** transactions/sec and potentially more than **100 million** transactions per second. Jun 3, 2018
- **Decentralize** complete scenario to increase availability and overcome single point failure.

REFERENCES

1. Dorri, Ali et al. "Blockchain in internet of things: Challenges and Solutions." *CoRR* abs/1608.05187 (2016): n. pag.
2. R. Bhattacharya, M. White, and N. Beloff, ''A Blockchain based peer-to-peer framework for exchanging leftover foreign currency,'' in Proc. Comput. Conf., Jul. 2017, pp. 1431–1435.
3. Beck, Roman; StenumCzepluch, Jacob; Lollike, Nikolaj; and Malone, Simon, "Blockchain – THE GATEWAY TO TRUST-FREE CRYPTOGRAPHIC TRANSACTIONS" (2016). *Research Papers*. 153.
4. Hernández-Ramos, José L., et al. "Distributed capability-based access control for the internet of things." *Journal of Internet Services and Information Security (JISIS)* 3.3/4 (2013): 1-16.
5. Dorri, Ali, et al. "Blockchain for IoT security and privacy: The case study of a smart home." *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on*. IEEE, 2017.
6. Yli-Huumo, Jesse, et al. "Where is current research on Blockchain technology? —a systematic review." *PloS one* 11.10 (2016): e0163477.
7. Liu, Jing, Yang Xiao, and CL Philip Chen. "Authentication and access control in the internet of things." *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on*. IEEE, 2012.
   Ouaddah, Aafaf, Anas AbouElkalam, and AbdellahAitOuahman. "Towards a novel privacy-preserving access control model based on Blockchain technology in IoT." *Europe and MENA Cooperation Advances in Information and Communication Technologies*. Springer, Cham, 2017. 523-533.
8. Mahalle, Parikshit N., et al. "Identity authentication and capability-based access control (iacac) for the internet of things." *Journal of Cyber Security and Mobility* 1.4 (2013): 309-348.
9. Roman, Rodrigo, Jianying Zhou, and Javier Lopez. "On the features and challenges of security and privacy in distributed internet of things." *Computer Networks* 57.10 (2013): 2266-2279.
10. Sun, Jianjun, Jiaqi Yan, and Kem ZK Zhang. "Blockchain-based sharing services: What Blockchain technology can contribute to smart cities." *Financial Innovation* 2.1 (2016): 26.
11. https://www.owasp.org/index.php/Top_Iot_Vulnerabilities
12. https://circuitdigest.com/microcontroller-projects/iot-based-patient-monitoring-system-using-esp8266-and-arduino
13. https://www.uk.sogeti.com/content-hub/blog/iot-security-using-Blockchain/
14. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/Blockchain-the-missing-link-between-security-and-the-iot
15. https://www.tripwire.com/state-of-security/security-awareness/Blockchain-helping-secure-iot-technology/
16. https://digiconomist.net/ethereum-energy-consumption
17. https://etherscan.io/chart/difficulty
18. H. Gross; M. Holbl, D. Slamanig, and R. Spreitzer, "Privacy-Aware Authentication in the Internet of Things," Cryptology and Network Security. Springer International Publishing, pp. 32-39, 2015.
19. Huckle, Steve, et al. "Internet of things, Blockchain and shared economy applications." *Procedia computer science* 98 (2016): 461-466.
20. Beck, Roman, et al. "Blockchain-the Gateway to Trust-Free Cryptographic Transactions." *ECIS*. 2016.
21. Ukil, Arijit, Soma Bandyopadhyay, and Arpan Pal. "Iot-privacy: To be private or not to be private." *Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on*. IEEE, 2014.

AUTHORS PROFILE

Dr. Premanand P Ghadekar /http://orcid.org/0000-0003-3134-137X He received Ph.D. degree from SGBA University, Amravati. He completed M.Tech degree in Electronics (Computer) from College of Engineering, Pune in the year 2008. He received BE degree in Electronics and Telecommunication Engineering from Government College of Engineering, Amravati, in 2000. In 2003, he joined the Department of Computer Engineering, Vishwakarma Institute of Technology, Pune, Maharashtra, India. He is presently working as an Associate Professor and Head of Information Technology Department. His areas of research are IoT, Machine Learning, Image Processing, Dynamic Texture Synthesis and Embedded System. He has contributed 10 papers in International conferences, 8 paper in International Journals and 2 papers in Springer book series. He is a life member of ISTE, member of IEEE. He has received research grants of two lakhs from BCUD Pune in March 2011.

MrNiket Subhash Doke (Research Scholar) He is currently pursuing BTech in Information Technology from Vishwakarma Institute of Technology. He has completed internship at Chainworks Digital LLP as Associative Blockchain System Engineer and is currently an intern at Vmware. His interests include Blockchain, Machine Learning and Artificial Neural Network.

Ms. **Sushmita Rajendra Kaneri (Research Scholar)** She is currently BTech in Information Technology from Vishwakarma Institute of Technology. She is interested in Blockchain technology and have completed her internship at Chainworks Digital LLP as Associate Blockchain Developer and is currently interning at vCreaTek LLC as Technology Intern.

Ms**. Varsha Jha (Research Scholar)** She is currently pursuing BTech in Information Technology from Vishwakarma Institute of Technology. She has completed in-house internship at Vishwakarma Institute of Technology in Internet of Things. Her interests are Blockchain, Internet of Things and Machine Learning.