Practical Byzantine Fault Tolerance based Security in IoT

[1]Nadiya Zafar, [2]Ashish Khanna, [3]Shaily Jain, [4]Zeeshan Ali, [1]Jameel Ahamed
[1]Department of CS&IT, Maulana Azad National Urdu University, Hyderabad INDIA
[2]Department of CSE, Maharaja Agrasen Institute of Technology, New Delhi INDIA
[3]Faculty of Computing, Engineering and Science, University of South Wales, UK
[4]University of Glasgow, UK
nadiyazafar5@gmail.com, ashishkhanna@mait.ac.in, shally.jain@southwales.ac.uk,
ali.zeeshan@glasgow.ac.uk, Jameel.shaad@gmail.com,

Abstract:

With the emergence of Internet of Things, massive amount of data is produced, processed, propagated and stored each and everyday. These IoT devices are built only to fulfil the aimed requirement with very limited resources. As a result, their security and privacy are not given as much thought. With such limited resources, implementing any system for the privacy and security issues of IoT devices is a difficult and critical undertaking. However, with the advent of Blockchain technology, adding security mechanisms in IoT systems no longer seems like a pipe dream. In this paper, we conducted numerous experiments to determine that pBFT is the best appropriate algorithm for securing IoT systems. The blockchain concept is utilized with pBFT in a similar way to Zilliqa and Hyperledger for IoT security. As a result, data integrity and authenticity would be ensured by detecting and preventing security breaches using the said algorithm.

Keywords: pBFT, data security, heterogeneous data, consensus algorithm, device certification

Introduction:

IoT gradually evolved from the combination of wireless technologies, microelectromechanical systems (MEMs), microservices and the Internet. It evolved from machine to machine communication and elevating M2M toward one more step ahead. IoT is a sensor network of billions of smart devices which connects human, system and other applications to gather and share data.

New emerging technologies have an impact on the world. Hence, there is a plethora of intelligent objects around us, making our lives easier and more comfortable[1].According to a Cisco networking survey, there are more smart devices than people in our world today. A growing number of people are connected to the Internet in some way, 24 hours a day, seven days a week; using three, four, or more smart devices. Smartphones, exercising and health monitors, and other similar devices may fall into this category. The world's population is 7.4 billion of people. By 2020, 30 billion devices will be connected to the internet[2]. When informationis exchanged and communicated through various information sensing devices, over a network, by agreeing upon some protocols; then this whole system is referred to as Internet of Things.Its aim is to intelligently identify, track down, monitor, and manage things[3].In layman's language, IoT meant for connecting devices over the internet, having limited abilities. The Things in IoT are the devices that can sense, monitor and actuate[4]. This unique connection of real devices has highly speed up the data gathering, summation and sharing process with other devices, giving emergence of IoT application in various new fields; such as medical field, smart housing and so on [5].However, mostly suchkind of devices and applications are not framed for surviving cyber-attacks, which raises slewof securityand privacy concerns in IoT networks such as confidentiality, authentication,data integrity, access control, and secrecy. All this, giving rise to vulnerability towards cyber theft

and breaches. Anonymity, privacy, trust, and liability are some other important security requirements[6].Security in IoT devices is a trending issue.
IoT connecting billion of devices and involving the use of billion of data points (nodes), all of which require security. Because IoT devices are closely connected, if intruders will exploit one vulnerability can manipulate all the data. Hackers are not the only threat to the IoT, privacy is also a major concern for IoT users. Companies manufacturing these IoT devices could use or leak personal dat of use. Basically, any smart device go through three life stages: manufacturing, installation and operational stage [7]. If at any stage of life there has been security flaws in smart devices it can cause major concern for privacy of user.On a daily basis, attackers and intruders target IoT devices. According to an assessment, seventy percent of IoT objects are easier to hack. As a result, an effective mechanism is critical for protecting internet-connected devices from hackers and intruders [8].

The flow of information must be secure in terms of integrity,confidentiality,non-repudiation, andauthentication.Therefore, we need a mechanism to protect IoT communication protocols from threat of attack. Because of dynamism, scalability, heterogeneity, limited resource availability in the IoT devices; its designation and implementation become very challenging for meeting allsecurity requirements. Hence, we require a system that will be compatible with such limited environment. The decentralized nature of blockchain technology is relevant for IoT system but most of the consensus algorithm requires much computational energy. While, pBFT uniquely don't require much computational power and take less time to reach consensus.pBFT is a consensus algorithm that reaches consensus even when some faulty nodes present in the system [9]. pBFT provides authenticity through consensus and integrity through keeping system alive [10]. pBFT gives priority to the nodes with high reliability for intrusion detection and identify them, all the nodes present in the network are available at the end of detection[11].

Advantages of pBFT:

a) Efficiency: In comparison with other consensus algorithm pBFT can reach distributed consensus without solving complex computational mathematics.
b) Transactional Finality: Multiple times confirmation is not required, like all other (proof of consensus) algorithms after finalization and approval.
c) Less recompense variance

Most prominent problems are limited computational resources of IoT devices and strict requirements for power consumption. pBFT doesn't requirerich computational resources, hence it can be used for the devices with limited resources.

Related Work

Within a network when smart objects are communicating and exchanging data, if any of it fails or attacked the whole system is jeopardized[6]. Here are some major security concerns:

A. Data Integrity: The data remains accurate during its transmission between nodes. For instance, it can be a severe problem, if the eve alters the data and orders to halt the production in any manufacturing organization[12].
B. Data Confidentiality: Data should remain private between shared nodes. Except for the sender and receiver, no one else should have access to the data. For instance, if infrastructure data is compromised, roads and bridges may be destroyed, and security may be jeopardized.
C. Data Authenticity: The authenticationensures that the data received is genuine and trustworthy. For example, the patient's parameters are transmitted to various medical centers. If somehow an eve altered this data, then patient's treatment may be jeopardized[13].
D. Data Availability: Data should be available to its concerned user. It is a major problem if the concerned user is not able to reach the data [6].

Beside all above mentioned issues there are much more challenges faced in handling with IoT system. Below are some of these major challenges:

1. Scalability: Innumerable connected IoT devices over-burdens the management of data access system. As a result, access control approaches should be scalable in terms of size, structure, and number of devices[14].
2. Heterogeneity: The Internet of Things connects objects with various fundamentalskills and application. As a result, the access control mechanisms are anticipated to facilitate interoperability between disparate objects[15].
3. Restricted Resources: Internet of Things (devices or nodes),mostly they are functioning without "screen" or even lacking any "user interface", depends upon battery power for functioning, commonly performing one task only [16].Because of the inconsequentiality of IoT devices, the computational and storage resourcesaccompanying them are constrained. As a result, an IoT access control model should be efficient and ideal in terms of overhead on devices and communication networks. Hence,theyare designed/equipped/deployed with limited computing and networking capability [17].
More than this, many kinds of devices communicate using several networks for IoT services. That means there can be many more security issues for the privacy of users and on the network layer. So, some other security concerns of IoT are: -
1) End to End Data life cycle protection: Data are gathered from many devices which are connected with each other and instantly passes onto other devices. Therefore, a complete structure needed to protect data throughout its life cycle.
2) Visible security and privacy: The majority of security and privacy issues are caused due to user's misconfiguration. It is necessary to choose security and privacy strategieswhich can be applied inevitably[6].
Recently, technical issues are resolved by extending and practicing wireless communication technologies, IoT model has to deal with hurdles associated security of IoT devices over the constrained environments [18].
Recent Internet security protocols depends upon a popular and trusted cryptographic algorithm: the Advanced Encryption Standard (AES) block cipher for confidentiality; the Rivest-Shamir-Adelman (RSA) asymmetric algorithm for digital signatures and key transportation; the Diffie-Hellman (DH) asymmetric key agreement algorithm and the SHA-1 and SHA-256 secure hash algorithms[19]. This suite of algorithms is supplemented by a set of emerging asymmetric algorithms, known as Elliptic Curve Cryptography (ECC)[20]. Because resource-constrained IoT devices lack computational power, general public key cryptosystems such as RSA are ineffective because they are slow and consume more power. Elliptical Curve Cryptography (ECC), on the other hand, is lightweight and has proven to be a suitable candidate for use in IoT networks [21]. In the IoT, the use of time stamps can protect data and serve as evidence that, data in the IoT are genuine, as they can be traced back to a particular time, making sure that the information are not tampered [22]. It is also very difficult to implement programming over IoT devices [23].

As the IoT system is growing rapidly its security issues are getting attention and blockchain has been seen as a new option for its security by the researchers [22]. With the rapid growth of mobile internet financial era, combination of the Internet of Things and the blockchain technologies seems as the most obvious option. The extensive use of "blockchain application technology" in the global IoT application field is going to perform a progressively significant role in the future.
The ideology ofblockchain is built upon a distributed security network. Its mechanism recommends strong data protection as well as protection from tampering [24]. Unlike used in

Bitcoin, blockchain data structure can be used in general as a data structure for storage. Liketransactions, any other data payloads can be used as the chain of block [25]. The blockchain's characteristics include: forgery, data encryption, and decentralization allowing it to execute and store confidential information, prevent data loss and ensure the security of IoT applications at various stages [23][24]. Because of properties such as immutability and irreversibility, blockchain is the most efficient data security and privacy technology available[26].
The blockchain's decentralized, trustworthy, and autonomous nature can significantly improve the security and privacy of ever-expanding IoT networks. Because IoT devices are the physical world contact points, combining blockchain and IoT will allow for the development of new applications as well as the transformation of existing systems [21].
Blockchain technology is preferred when information security and confidentiality are the network's top priorities. Implementing blockchain in IoT allows for more efficient access control. The most vital feature affecting IoT blockchain throughput is the consensus mechanism [27]. The consensus algorithm is at the heart of Blockchain technology because it ensures the network's integrity and security. It is a protocol that allows block-chain network nodes to reach a standard agreement on the current state of the ledger's records. Different block-chain platforms use different algorithms to reach consensus, and they all operate and execute differently [28].

Although, presently no blockchain and consensus protocol might concurrently meet both the security and scalability requirements[29].Most organizations still lack tools for tracking active keys, and roughly quasi-firms experience complications in implementing encryption and take it aschallenging because of unclear proprietorship and shortage of experts [30].
But for applying blockchain to the IoT environment, some challenges are most to be fulfilled.
•Latency: In permissionless blockchainframeworks it takes between 1 to10 minutes to reach consensus. In permissioned blockchain it contracts uptomilliseconds.
• Applicability: Generally, there are different kind of devices that are connected within an IoT system. So, it is very difficult to choose a blockchain framework which will be supported by all devices[31].
It is required to useasuchblockchain architecture which allow unified and ascendable movement of data from the IoT device to the consensus protocol [29].

Blockchain technology, in conjunction with IoT, cloud computing, big data, and machine learning, can provide a comprehensive solution to these problems [12].Smart contracts, on the other side, have the ability to supplement existing technicalmethods for resolving security challenges. Whereas Blockchain integrallyviolates its distinguishing characteristics such as immutability,traceability, and authenticity[32]. Smart contracts, then again, make use of adaptable features such as their customizable nature, similarities with broadly used scripting languages, and Turing-completeness of their scripting language. The majority of researches indicates that the application of smart contracts with presentsubstructurestrengthening the security solutions provided to IoT environments [33]. For the proper function and integration of various IoT devices, there is a need of huge distributed system for storing and transmitting data [34]. Because of the ever-increasing number of IoT devices, data vulnerability is a constant risk. Existing centralized IoT ecosystems have raised security, privacy, and data use concerns. A decentralized ID and access management (DIAM) system for IoT devices is the best solution to these concerns, and that Hyperledger is the best technology for such a system [35].Fault tolerant consensus protocols play a vital role in establishing trustworthiness of a system in spite of the chances of node failures [36].

Table 1: Comparison between all proof of consensus algorithms:[37]

Properties	PoW	PoS	pBFT
Integrity management of nodes	Open	Open	Permissioned
Saving Energy	No	Partial	Yes
Tolerance	<51%	<51%	<33.3%
Blockchain	Private	Private	Public[37]

A milestone paper by Lamport et al. firstly presented the idea of Byzantine failure. They proposed their ideology through the case of Byzantine generals, whose troop targeting a castle of rival. Upon seeing the enemy, the Generals communicate with each other and agree over a plan of action (consensus) – either to attack or retreat. If they attack altogether, they succeeded; if none of them attack, they will survive for other day. If some of the general's attack, then the generals will not survive. They communicate through messages. The challenge is that one or more of the generals can deceive and passes onerratic messages to interrupt the faithful generals from reaching consensus[38]. All consensus algorithm requires two phase one for request and other for reply while pBFT requires three phase for massive communicaton[36].pBFT is the most popular algorithm providing tolerance under malicious attack[39].

Table 2: A comparison table for BFT and pBFT:[40]

BFT	**pBFT**
Consensus algorithm	Consensus algorithm
Group of nodes finds consensus; some nodes could be malicious.	Generate consensus in malicious environment.
Less efficacy to operate in adversarial environment.	More efficacy to operate in adversarial environment.

Research gaps

Through literature survey, we come to the point that whatever work has been done over security issue of IoT devices; various proof of consensus algorithms has implemented over IoT security devices for data privacy at various aspects data confidentiality, authenticity, integrity, availability and so on. However, all have some limitation due to its heterogeneous architecture. There is also not so much talk over device certification.

Problem Statement

- Implementing Practical Byzantine Fault Tolerance algorithm to improve integrity and authenticity of data during its propagation from one node to another over the IoT system.

Contribution and Result:

The proposed methodology follows the approach "practical Byzantine Fault Tolerance Algorithm(pBFT)", a consensus algorithm for secure propagation of data introduced in by Barbara Liskov and Miguel Castro. For checking whether nodes are reliable or not, protocol uses timestamp from IoT devices [27].It is an advancement in Byzantine Fault

Tolerance(BFT) algorithm, yielding more efficient result than BFT for distributed systems. The highest number of malicious nodes should be less than or equal to 1/3rd of total nodes for working of Byzantine Fault system[41].Request of all clients must reach to the nodes and concurrent issue doesn't arises. In the process if leader node fails immediately another leader is selected [42]. The system becomes more secure as the number of nodes grows.

Execution phases seems be like this:

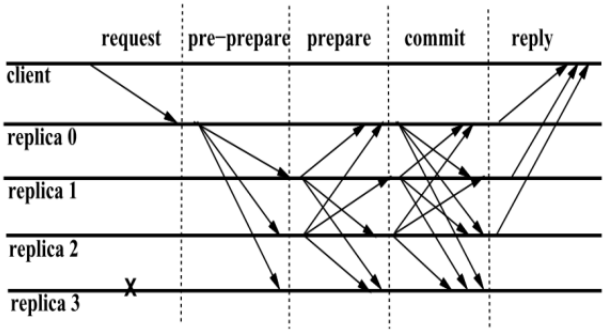


Fig. 1Working phases of pBFT [9]

Requirements will be: a) increment in the number of nodes will be adopted.b) Failure of any nodes doesn't affect the system.
pBFT consensus cycle are divided into four stages:
1. Request sent to primary node by client.
2. Requests are broadcasted to all secondary nodes by primary node.
3.Then nodes execute the service requested send a respond to the client.
4. When *n+1* similar responds received by the client from various node of the network, then the request is said to be completely served. Where *n* is the total number of nodes.

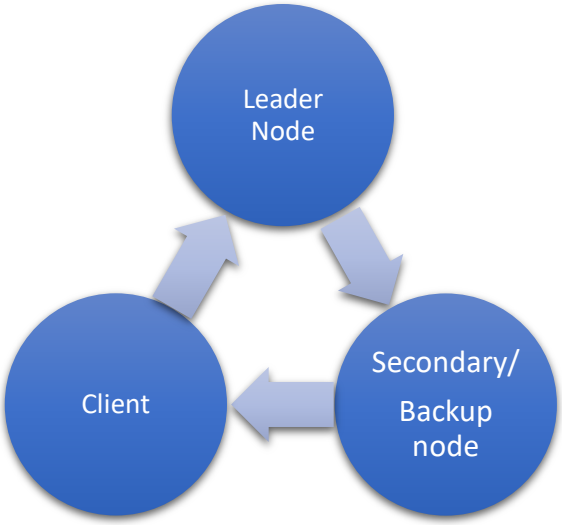


Fig. 2. Pictorial representation of algorithm

Algorithm

While client sends request to leader node

do leader node broadcast it to all secondary nodes
if $n>2/3^{rd}$ authentic
then agree
else if$Q<= N-f$
then live
else*if* $Q>N/2$
then safe
else: malicious
if leader node is malicious
then change the leader node
Where*m+1* replies should be received from secondary nodes
Endif

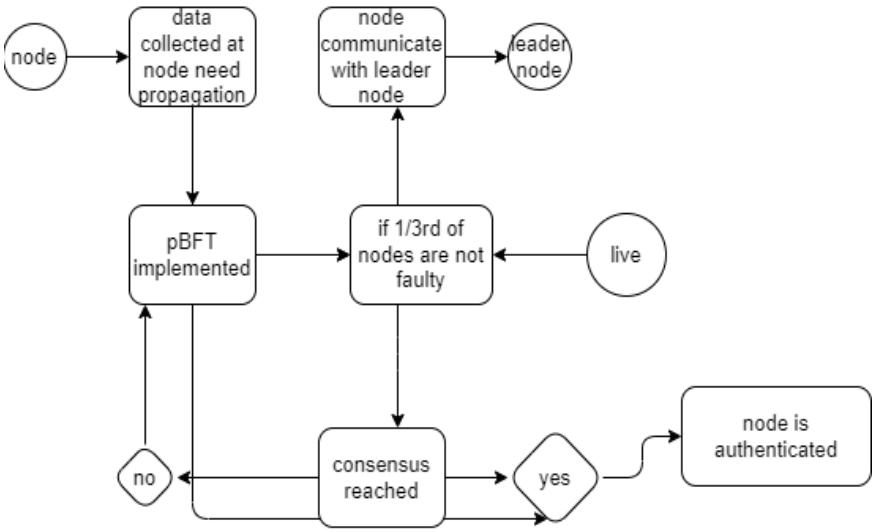


Fig. 3 Block diagram of proposed work

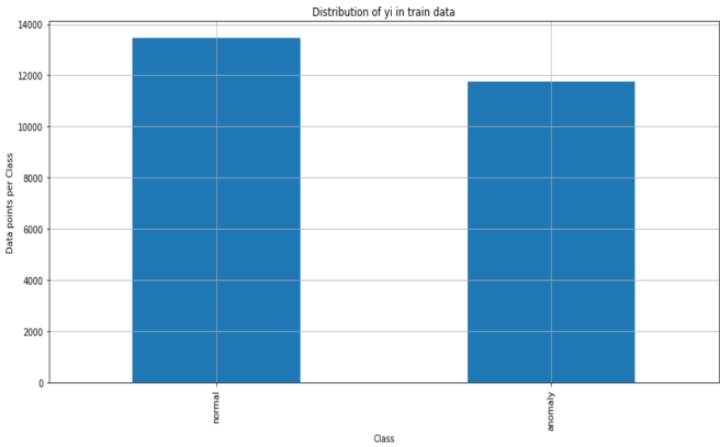


Fig.4Dividing dataset into two class normal and anomalous

Theorem

Here for maintaining integrity of data we have used hash function. The message digest is created at the sender node and is sent with the message to the receiver node. To check the

integrity of a message, the receiver generates a hash function and compare the new message digest with the one received. If they both are same then only data of one node is approved to pass onto other.

$$h(y) = h(x)\text{……..(1)}$$

Then the consensus is reached and a message like this will appear and the propagation of data will be approved without malice.

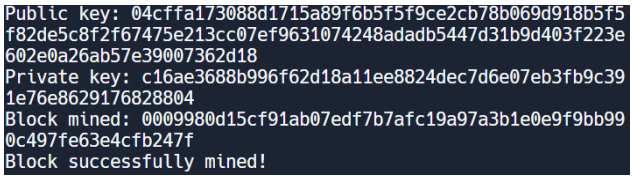


Fig 5integrity of nodes approved

Rules:[43][39]

1. Client must receive *f+1* replies; where f is the number of faulty nodes
2. *More than two-third* nodes should be authentic

   Agree = 3f + 1
3. Liveness: *Q<= N-f*where Q is a constant for Quorum consensus

   where N is the total number of nodes

   Safety: *Q> N/2*

Result

At nodes data collected from various sensors are stored and when they are propagated from one node to another then pBFT performs its role and check whether the information passingthrough are authentic or not, if they are not authentic and fails to fulfil the rule of *3f+1* consensus they simple breaks them without disturbing the system. So, it is providing two step security.

Liveness and safety are guaranteed by algorithm until unless *n-1/3*out of n nodes are faulty, which indicates that client will receive correct replies for their request node.

Firstly, we have done simpleimplementation on replit(a coding platform) for algorithm pBFT then we have used the Contiki simulator (simulator for IoT) for real time simulation. For safety mechanism we have used cryptographic public and private key. Here, we are excluding the details of implementation part due to space issue. In this paper we are assuming that client will only send the next request until unless first one is served. If they will send requests one after other spontaneously, that will result into congestion problem.

The algorithm will provide safety only when non-malicious nodes reach consensus. To maintain liveliness, if leader node is examined malicious, another node is urgently appointed as leader. Many of the system succeeded in implementing safety but fails to maintain liveness. But this system is giving solution for both simultaneously. To maintain liveliness its following two approach: - first one is the rule of $1/3^{rd}$ node and second one is changing leader node.The significance of pBFT is that, it will keep the system alive until unless there is reliable number of nodes, which are greater than the number of faulty nodes.

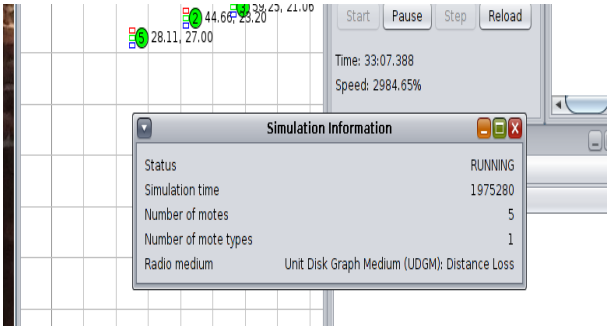


Fig 6: real time simulation

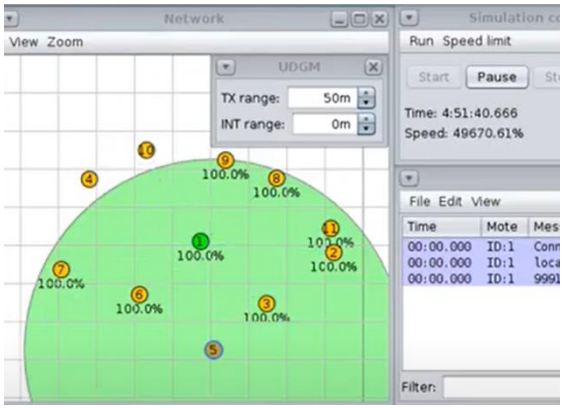


Fig 7: 10 nodes communicating with each other

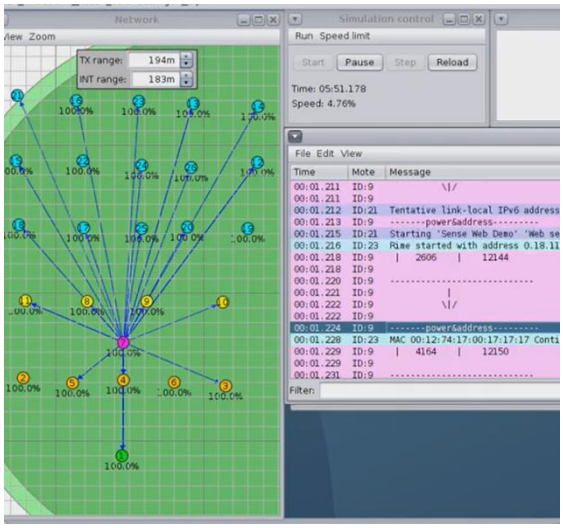


Fig 8:25 nodes communicating with each other

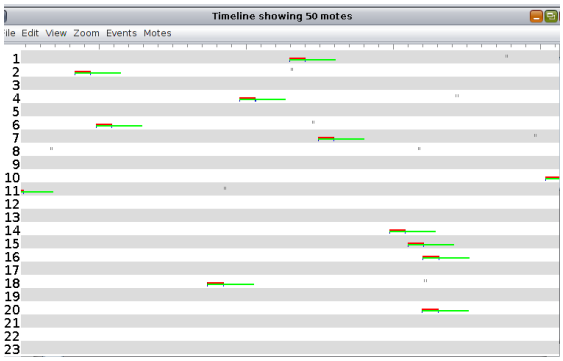


Fig 10 Timeline of 50 nodes

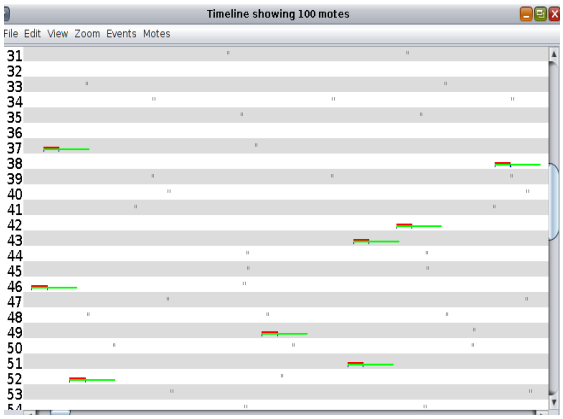


Fig 9 Timeline of 100 nodes

Our performance evaluators are number ofnodes, speed & simulation time in milliseconds. The number of nodes is showed as *[1+....n]* where *1* denotes leader node and ....+*n* denotes other nodes. The time in milliseconds is showing the time required to communicate one node to another in real time.
On the real time simulator, green region is the region of strong connection and gray is of weak connection. The node having sky blue color is the leader node and rest of nodes of green colors arebackup/secondary nodes.

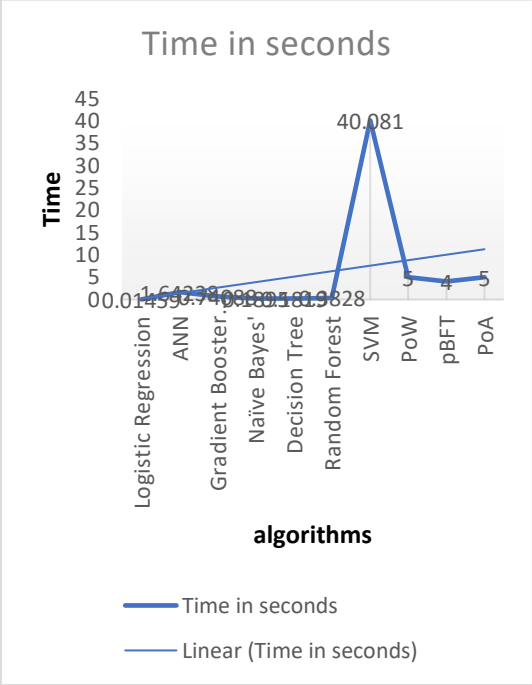
Earlier IoT was secured through ML algorithm but now researchers and scientists started using blockchain technologies for the security of IoT devices. IoT network is an ecosystem in which variety of devices exist. It is almost impossible to train data and provide security for all kind of sensors/gadgets on the other hand blockchain is providing security using cryptographic techniques and consensus agreement rule over the network. There is a brief comparison of these two technologies:

Table 3: Comparison table of ML and Consensus algorithms [44]:

Technique	**Time in seconds**	**Prior data training**	**Cryptographic method used**
Logistic Regression	0.01459	Yes	No
Advanced Neural Network (ANN)	1.64238	Yes	No
Gradient Booster Classifier	0.74088	Yes	No
Naïve Bayes’	0.1895	Yes	No
Decision Tree	0.1819	Yes	No

Random Forest	0.3828	Yes	No
Support Vector Machine (SVM)	40.081	Yes	No
Proof of Authority (PoA)	5-8	No	Yes
Practical Byzantine Fault Tolerance (pBFT)	4-26	No	Yes
Proof of Work (PoW)	5-8	No	Yes

Note: For machine learning algorithm time evaluated is testing time in seconds and for consensus algorithm it is block validation time.
Note: Once Block validation executed nodes can communicate with milliseconds.



Graph 1 graphical representation for comparison of various algorithms

Furthermore, comparing Practical Byzantine Fault Tolerance algorithm with another consensus algorithms and analyzing why they suitable for IoT.

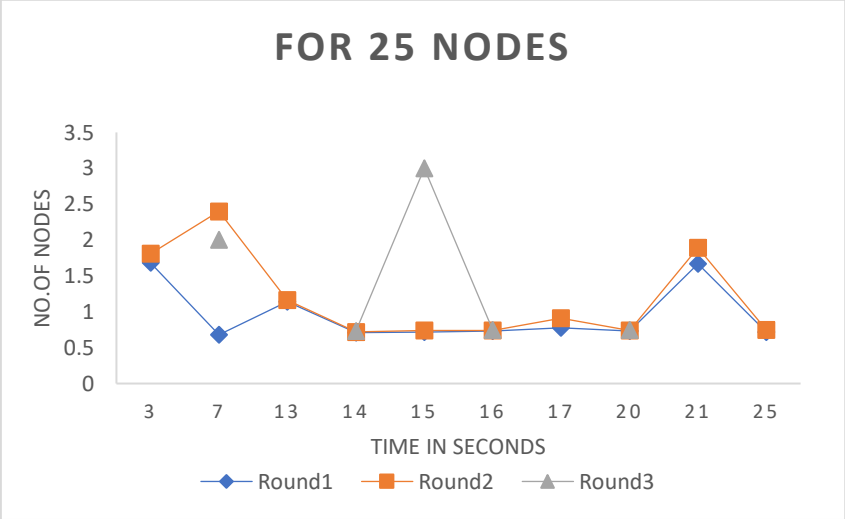
Time: Time utilized for block validation
Energy consumption.
Mechanism: Protocol or cryptographic technique used for reaching consensus.

Table 4: Comparison table of various consensus algorithm [40][45]

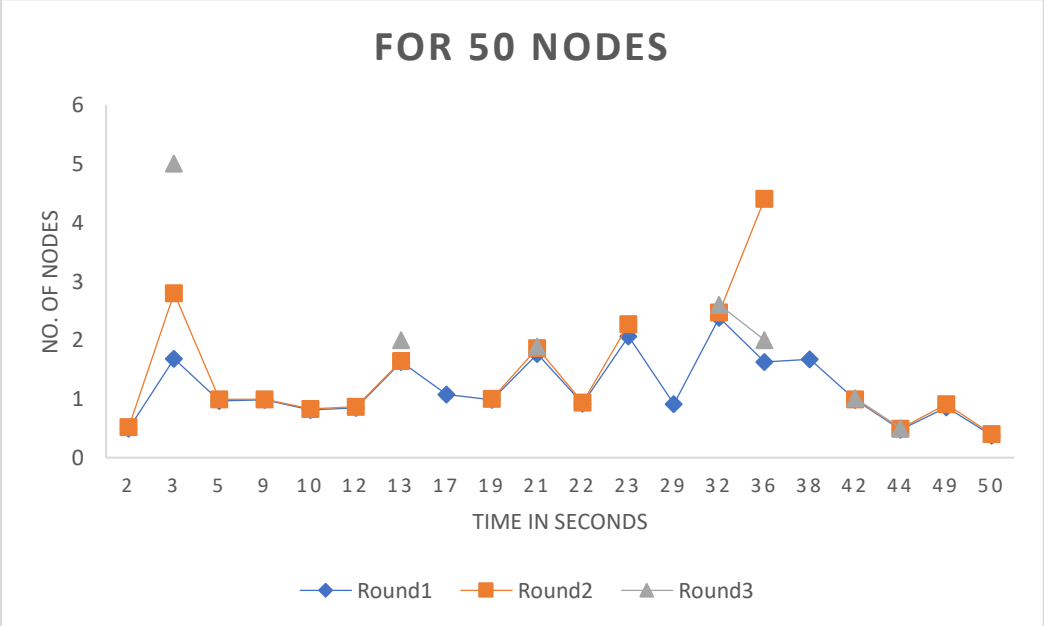
Algorithm	**Time in seconds**	**Energy Consumtion**	**Mechanism**
Proof of Work (PoW)	5-8	High	Based on computing power
Proof of Stake (PoS)	12	Relatively low	High stakes nodes have the right to account
Proof of Authority (PoA)	4-5	High	Validators that help to reach consensus
Byzantine Fault Tolerance (BFT)	4-10	Relatively low	Reach agreement based on value

Practical Byzantine Fault Tolerance	4-26	Low	Using majority rule

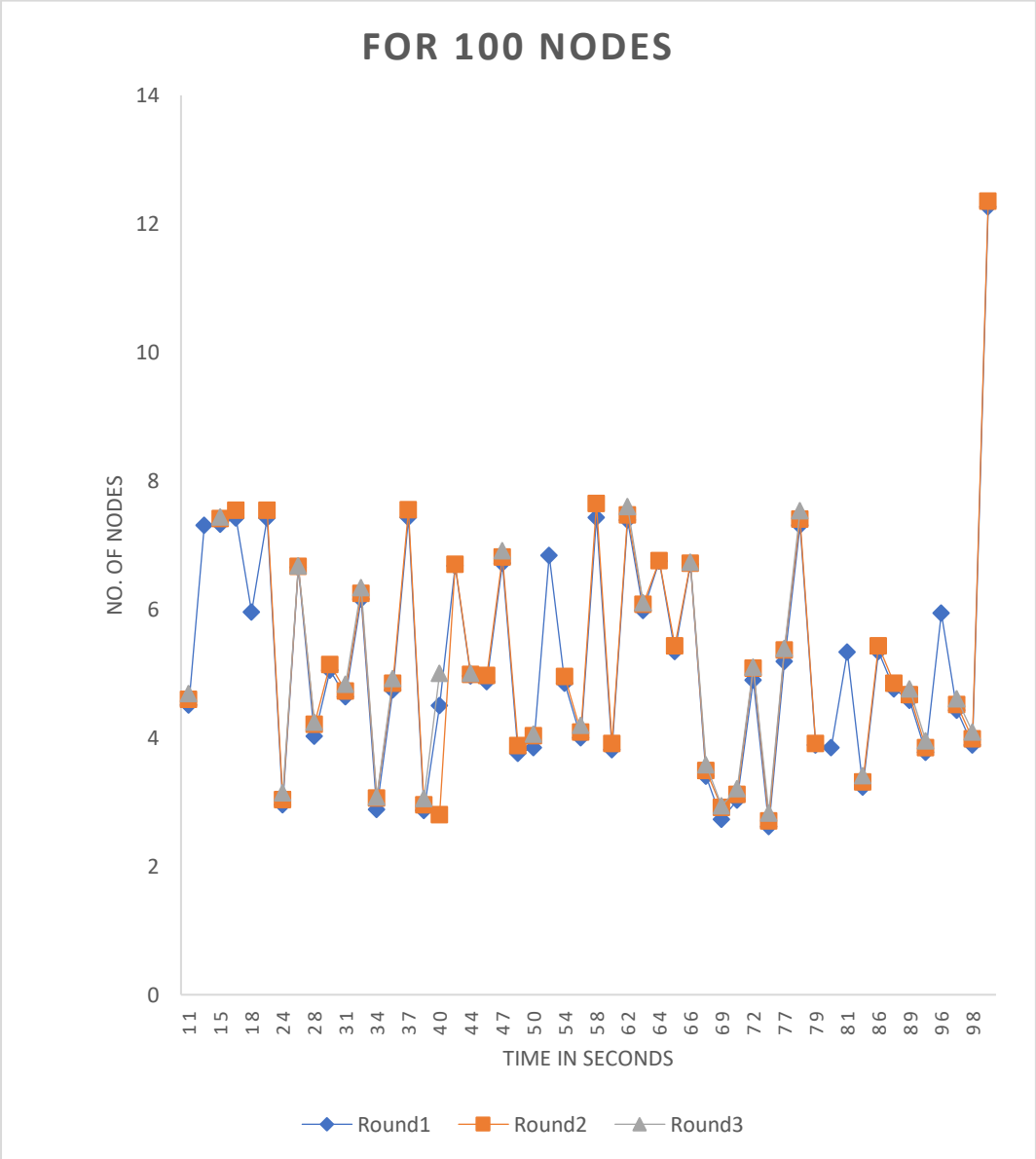
Technique	Time in seconds	Speed	Power Consumption
RSA	6 for 100 nodes	slow	High
Diffie-Hellman	4.6 for 100 nodes	slow	High
ECC	4 for 100 nodes	fast	Comparatively low
pBFT	3 for 100 nodes	fast	low



Graph 2



Graph 3

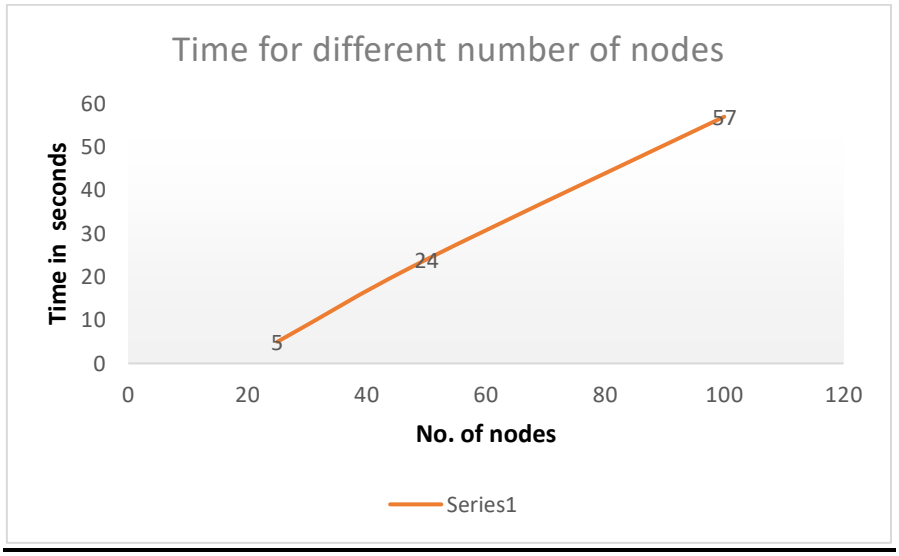


Graph 4

Table 5: pBFT on different no. of nodes

Practical Byzantine Fault Tolerance Algorithm		
Time in seconds	For 25 nodes	11
	For 50 nodes	24
	For 100 nodes	57

average time = (11+24+57)/3
54 secs……(2)



Graph 5

Security of data is a major issue in IoT domain. There is a high risk of privacy breaching and data stealing during data propagation through IoT layers. Using pBFT, at network layer of IoT would reduce chances of its breaching and stealing. Till now, in Intrusion Detection System for IoT there is lack of accuracy in trialoutput and some inconsistency issues. However, pBFT would efficiently resolve the issues that exists in the existing mechanisms [11]. Although, the optimistic fast path could be achieved only when there is not aletdown. Else, the proprietiesbehaves like randomized consensus having congestion issue [46].

However, IoT devices like sensors go through various life stages discussed above. If there is any issue in sensors at manufacturing stage, it can cause great damage and end upwith interoperability issue[47]. The best solution for this issue is the device certification. Certification could be based on some standard norms followed by manufacturing industry or provided by government. If any device certified by government organization, then must follow privacy rules and regulation of that country and will be more trustable by the customers. On the other hand, if a device is certified could be claimed and challenged for their issues.

Conclusion and Future Scope

Based on various analysis and comparisons we reach on a result that pBFT is the most suitable algorithm for the security of IoT as it is using cryptographic technique, time consumed is low, energy consumption is also low and most important thing is that the system remains live despite of having malicious nodes.In the paper, the proposed method is concerned about data integrity and authenticity, through practical Byzantine Fault Tolerance (pBFT) providing an approach for more safe and secure data propagation along IoT devices. This paper also stressing over the certification of IoT devices. Certification of IoT devices; resolves most of the problem of sensor interoperability.pBFT may provide a way for data

security in IoT; but it will be very hard to implement it in every case due to heterogeneous nature of Internet of Things(IoT). On our experiment basis if data is propagated with huge velocity, then system may not crash but congestion would happen. In future we will work over this propagation delay.

REFERENCES:

[1] M. Husamuddin and M. Qayyum, "Internet of Things: A study on security and privacy threats," *2017 2nd Int. Conf. Anti-Cyber Crimes, ICACC 2017*, no. October, pp. 93–97, 2017, doi: 10.1109/Anti-Cybercrime.2017.7905270.

[2] T. Cisco and A. Internet, "Cisco: 2020 CISO Benchmark Report," *Comput. Fraud Secur.*, vol. 2020, no. 3, pp. 4–4, 2020, doi: 10.1016/s1361-3723(20)30026-9.

[3] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with China Perspective," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 349–359, 2014, doi: 10.1109/JIOT.2014.2337336.

[4] P. Nespoli, D. Díaz-López, and F. Gómez Mármol, "Cyberprotection in IoT environments: A dynamic rule-based solution to defend smart devices," *J. Inf. Secur. Appl.*, vol. 60, no. May, 2021, doi: 10.1016/j.jisa.2021.102878.

[5] A. Hamid Lone and R. Naaz, "Reputation Driven Dynamic Access Control Framework for IoT atop PoA Ethereum Blockchain."

[6] K. Kasemsap, "Internet of Things and Security Perspectives," *Secur. Internet Things*, vol. 5, no. 1, pp. 1–20, 2019, doi: 10.4018/978-1-5225-9866-4.ch001.

[7] C. Lu, "Overview of Security and Privacy Issues in the Internet of Things Abstract : Keywords : Table of Contents," pp. 1–11, 2014.

[8] M. B. Yassein, W. Mardini, and A. Al-Abdi, "Security Issues in the Internet of Things," vol. 8, no. 6, pp. 186–200, 2017, doi: 10.4018/978-1-5225-3029-9.ch009.

[9] M. C. and B. Liskov, "Practical Byzantine Fault Tolerance Miguel," *Juv. Delinq. Eur. Beyond Results Second Int. Self-Report Delinq. Study*, no. February, pp. 359–368, 2010.

[10] Y. Meshcheryakov, A. Melman, O. Evsutin, V. Morozov, and Y. Koucheryavy, "On Performance of PBFT Blockchain Consensus Algorithm for IoT-Applications with Constrained Devices," *IEEE Access*, vol. 9, no. June, pp. 80559–80570, 2021, doi: 10.1109/ACCESS.2021.3085405.

[11] L. Li, Y. Chen, and B. Lin, "Intrusion Detection Analysis of Internet of Things considering Practical Byzantine Fault Tolerance (PBFT) Algorithm," *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021, doi: 10.1155/2021/6856284.

[12] C. Hosmer, "IoT Vulnerabilities," *Defending IoT Infrastructures with Raspberry Pi*, pp. 1–15, 2018, doi: 10.1007/978-1-4842-3700-7_1.

[13] E. Bouscaren, "Elementary pairs of models," *Ann. Pure Appl. Log.*, vol. 45, no. 2 PART 1, pp. 129–137, 1989, doi: 10.1016/0168-0072(89)90057-2.

[14] A. Sultan, M. A. Mushtaq, and M. Abubakar, "IoT security issues via blockchain: A review paper," *PervasiveHealth Pervasive Comput. Technol. Healthc.*, vol. Part F1481, pp. 60–65, 2019, doi: 10.1145/3320154.3320163.

[15] Rachit, S. Bhatt, and P. R. Ragiri, "Security trends in Internet of Things: a survey," *SN Appl. Sci.*, vol. 3, no. 1, pp. 1–14, 2021, doi: 10.1007/s42452-021-04156-9.

[16] Inside Secure, "Iot Security Solutions White paper", Veritmatrix

[17] C. Wheelus and X. Zhu, "IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework," *IoT*, vol. 1, no. 2, pp. 259–285, 2020, doi: 10.3390/iot1020016.

[18] J. L. Hernandez-Ramos, M. P. Pawlowski, A. J. Jara, A. F. Skarmeta, and L. Ladid, "Toward a lightweight authentication and authorization framework for smart objects," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 4, pp. 690–702, 2015, doi: 10.1109/JSAC.2015.2393436.

[19] Azamuddin, "Rotation Project Title : Survey on IoT Security," [Online]. Available: https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_sec2.pdf.

[20] T. K. Goyal and V. Sahula, "Lightweight security algorithm for low power IoT devices," *2016 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2016*, no. September, pp. 1725–1729, 2016, doi: 10.1109/ICACCI.2016.7732296.

[21] K. P. Satamraju and B. Malarkodi, "A secured and authenticated internet of things model using blockchain architecture," *Proc. 2019 TEQIP - III Spons. Int. Conf. Microw. Integr. Circuits, Photonics Wirel. Networks, IMICPW 2019*, pp. 19–23, 2019, doi: 10.1109/IMICPW.2019.8933275.

[22] H. Zhang and W. Lang, "Research on the Blockchain Technology in the Security of Internet of things," *Proc. 2019 IEEE 4th Adv. Inf. Technol. Electron. Autom. Control Conf. IAEAC 2019*, no. Iaeac, pp. 764–

768, 2019, doi: 10.1109/IAEAC47372.2019.8997876.
[23] A. Kurniawan, R. Mayasari, and M. A. Murti, “Implementation of Cryptographic Algorithm on Iot Device’S Id,” *J. Sist. Cerdas*, vol. 01, no. 02, pp. 19–26, 2018.
[24] J. Zhang and Z. Li, “Design of internet of things information security based on blockchain,” *Proc. - 2020 3rd World Conf. Mech. Eng. Intell. Manuf. WCMEIM 2020*, pp. 114–117, 2020, doi: 10.1109/WCMEIM52463.2020.00030.
[25] A. Moinet, B. Darties, and J.-L. Baril, “Blockchain based trust & authentication for decentralized sensor networks,” pp. 1–6, 2017, [Online]. Available: http://arxiv.org/abs/1706.01730.
[26] D. Na and S. Park, “Fusion chain: A decentralized lightweight blockchain for iot security and privacy,” *Electron.*, vol. 10, no. 4, pp. 1–18, 2021, doi: 10.3390/electronics10040391.
[27] X. Yuan, F. Luo, M. Z. Haider, Z. Chen, and Y. Li, “Efficient Byzantine Consensus Mechanism Based on Reputation in IoT Blockchain,” *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021, doi: 10.1155/2021/9952218.
[28] P. Patil, M. Sangeetha, and V. Bhaskar, “Blockchain for IoT Access Control, Security and Privacy: A Review,” *Wirel. Pers. Commun.*, vol. 117, no. 3, pp. 1815–1834, 2021, doi: 10.1007/s11277-020-07947-2.
[29] B. Mackenzie, R. I. Ferguson, and X. Bellekens, “An Assessment of Blockchain Consensus Protocols for the Internet of Things,” *2018 Int. Conf. Internet Things, Embed. Syst. Commun. IINTEC 2018 - Proc.*, pp. 183–190, 2018, doi: 10.1109/IINTEC.2018.8695298.
[30] I. Kuzminykh, M. Yevdokymenko, and D. Ageyev, “Analysis of Encryption Key Management Systems: Strengths, Weaknesses, Opportunities, Threats,” *2020 IEEE Int. Conf. Probl. Infocommunications Sci. Technol. PIC S T 2020 - Proc.*, no. April, pp. 515–520, 2021, doi: 10.1109/PICST51311.2020.9467909.
[31] S. S. Seshadri *et al.*, “IoTCop: A Blockchain-Based Monitoring Framework for Detection and Isolation of Malicious Devices in Internet-of-Things Systems,” *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3346–3359, 2021, doi: 10.1109/JIOT.2020.3022033.
[32] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, “Applications of Blockchains in the Internet of Things: A Comprehensive Survey,” *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019, doi: 10.1109/COMST.2018.2886932.
[33] A. H. Lone and R. Naaz, “Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic literature review,” *Comput. Sci. Rev.*, vol. 39, p. 100360, 2021, doi: 10.1016/j.cosrev.2020.100360.
[34] Y. Meshcheryakov, A. Melman, O. Evsutin, V. Morozov, and Y. Koucheryavy, “On Performance of PBFT Blockchain Consensus Algorithm for IoT-Applications with Constrained Devices,” *IEEE Access*, vol. 9, no. April, pp. 80559–80570, 2021, doi: 10.1109/ACCESS.2021.3085405.
[35] A. Hyperledger and A. L. F. Edge, “Decentralized ID and Access Management (DIAM) for IoT Networks.”
[36] H. Goyal and S. Saha, “Practical Byzantine Consensus for Internet-of-Things.”
[37] V. Sharma and N. Lal, “a Novel Comparison of Consensus Algorithms in Blockchain,” *Adv. Appl. Math. Sci.*, vol. 20, no. 1, pp. 1–13, 2020.
[38] K. Driscoll, B. Hall, H. Sivencrona, and P. Zumsteg, “Byzantine Fault Tolerance , from Theory to Reality 1 What You Thought Could Never Happen,” *Thought A Rev. Cult. Idea*, no. 2, pp. 235–248, 2003, doi: 10.1007/978-3-540-39878-3_19.
[39] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, “A Scalable Multi-Layer PBFT Consensus for Blockchain,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 5, pp. 1146–1160, 2021, doi: 10.1109/TPDS.2020.3042392.
[40] I. Gorkey, E. Sennema, C. El Moussaoui, and V. Wijdeveld, “Comparative Study of Byzantine Fault Tolerant Consensus Algorithms on Permissioned Blockchains Supervised by Zekeriya Erkin Supervised by Miray Aysen,” no. April, pp. 1–11, 2020.
[41] J. Misic, V. B. Misic, X. Chang, and H. Qushtom, “Multiple entry point PBFT for IoT systems,” *2020 IEEE Glob. Commun. Conf. GLOBECOM 2020 - Proc.*, pp. 0–5, 2020, doi: 10.1109/GLOBECOM42002.2020.9322641.
[42] J. Misic, V. B. Misic, X. Chang, and H. Qushtom, “Adapting PBFT for Use with Blockchain-Enabled IoT Systems,” *IEEE Trans. Veh. Technol.*, vol. 70, no. 1, pp. 33–48, 2021, doi: 10.1109/TVT.2020.3048291.
[43] X. Liangchen, “Design and Implementation of Internet of Things Information Security Transmission Based on PBFT Algorithm,” *Proc. - 2020 Int. Conf. Comput. Eng. Appl. ICCEA 2020*, pp. 201–205, 2020, doi: 10.1109/ICCEA50009.2020.00051.
[44] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, “Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures,” *ACM Comput. Surv.*, vol. 53, no. 6, 2021, doi: 10.1145/3417987.

[45] H. Xiong, M. Chen, C. Wu, Y. Zhao, and W. Yi, “Research on Progress of Blockchain Consensus Algorithm: A Review on Recent Progress of Blockchain Consensus Algorithms,” *Futur. Internet*, vol. 14, no. 2, 2022, doi: 10.3390/fi14020047.

[46] P. Kuznetsov, A. Tonkikh, and Y. X. Zhang, *Revisiting Optimal Resilience of Fast Byzantine Consensus*, vol. 1, no. 1. Association for Computing Machinery, 2021.

[47] M. Noura, M. Atiquzzaman, and M. Gaedke, “Interoperability in Internet of Things: Taxonomies and Open Challenges,” *Mob. Networks Appl.*, vol. 24, no. 3, pp. 796–809, 2019, doi: 10.1007/s11036-018-1089-9.