iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VII **Month of publication:** July 2020

DOI: http://doi.org/10.22214/ijraset.2020.7032

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

Measuring Performance of Blockchain Enabled IoT over Edge Computing System

Sampada Desai[1], Sunilkumar Padhi[2]
[1, 2]*Capgemini Technology Services India Limited, Navi Mumbai, Maharashtra, India*

Abstract: ***In today's era there has been a huge demand in the automation space where most of the human tasks could be operated remotely. IoT (Internet enabled devices) makes it possible with the usage of sensors and gateways. The success of mission critical systems depends upon how quickly such devices respond. Edge computing can boost up the responsiveness of these devices by offloading certain computational tasks closer to these devices. Merging these technologies with blockchain makes this distributed system more secure and reliable. Our paper focuses on these technologies, their working and how well they complement each other when integrated. The main focus is to shed some light on the key metrics for measuring responsiveness of the system, the challenges encountered while performance testing such applications and to provide the possible solutions for the same. We have referred published literatures around these topics and collated insights under the hood. The main purpose of this paper is to maximize the ROI made on the testing activities of such complicated integrated system.***
Keywords: IoT; Edge Computing; Blockchain; Performance Testing; Distributed System; Tolerant Proof Network; Key Performance Indicators; Cloud Computing, IoT Gateway; Consensus, Proof of Work (PoW)

I. INTRODUCTION

The technology innovations of today are tomorrow's imperative. Currently we are on the cusp of system where the IoT objects amalgamate well with the blockchain network under edge computing topology. Before we directly jump into this integrated system, let us shed some light on each of these components individually.

A. IoT

1) Description: The Internet of Things is a technology that enables the devices to exchange the data with each other over the Internet to perform a particular task remotely. A 'thing' in IoT could be any device that has a unique identifier and can communicate over the network. IoT makes the device smart and extends its working capabilities making the human life easier. These devices need not have a high-end computing processor or huge storage. The bare minimum expectation from these IoT enabled devices is to transmit data over Internet and/or be able to perform the desired action. It could be something like controlling an air conditioning at home, turning off tubelights, bulbs or fan, closing the main door, windows or garage door through a mobile app from office or any other remote location.

2) Components

a) *Sensors*: It is used to continuously collect the raw data from the environment and send it through gateway. There could be more than one sensor embedded in the device that captures the data from various aspects making the device even smarter.

b) *Gateway*: It is a medium through which the data is transferred. This is mostly a wireless network. It ensures the interoperability of the connected devices and sensors.

c) *Cloud*: It is the main processing unit where the data is being analyzed and processed by implementing simple to complex algorithms. It has super computing power and huge memory for storage.

d) *User interface*: It is used to display the processed information in a meaningful dashboard with graphs/tables. It could also show alerts for actionable items. It helps users to monitor and control the IoT device remotely.

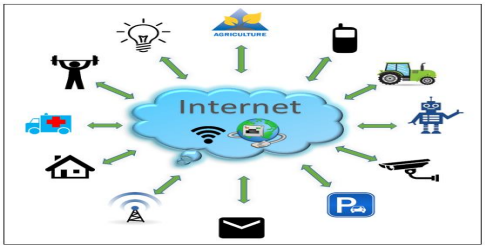


Fig. 1 Applications of IoT System

3) *Working of IoT*: Let us try to understand working of IoT through an example.

Consider a bank that is equipped with smart gadget like a door of the treasure room with NIR (for face detection) and proximity sensor (for object location).

a) The NIR and proximity sensors attached to the smart door continuously collects the data of nearby objects, wraps it to a single data packet and send it to the centralized server through the Gateway. These sensors are attached to a consistent power source and has wireless connection to the Internet.

b) Once the cloud server receives this data, the raw data is processed, and necessary information is analyzed.

c) Let's assume case#1 where the bank manager has forgotten to shut the door of treasure room. The algorithm under the hood detects this and triggers the necessary alarm to a mobile application. The bank manager gets notified of the open door. He then triggers a command to close the door remotely through the same mobile app. This command is sent to the cloud server. This is where person to machine communication takes place. The cloud server analyzes the command and sends the necessary signal to close the door immediately. The sensors on the door activates the levers and the door gets closed.

d) Let's assume case#2 where an unauthorized person attempts to access the treasure room. The NIR sensor captures the face recognition data and send it to the cloud server. The cloud server analyzes this data and flags this access as unauthorized. It then immediately triggers a security breach alarm and also notifies the bank manager through an interactive mobile app. This is where machine to machine communication takes place.

The usage of IoT devices in the recent years has grown exponentially. With this rapid use, a huge amount of data is being transmitted between the IoT device and the cloud. With the conventional cloud infrastructure, the processing and storing of these data has become too costly and time consuming. The communication between end terminals to the cloud needs to be much faster to meet the needs of the end user. At certain critical situations, a delay of a couple of second may lead to serious loss. This is where Edge computing plays an important role. Now let's understand what Edge Computing is and how it boosts the performance of IoT.

B. Edge Computing

1) *Description:* Rather than relying on a centralized cloud server which could be situated several miles away from the IoT device for data processing, a topology that allows the processing and data storage on premise is termed as Edge Computing. It focuses on performing maximum computing at the edge i.e. closer to the source that generates data or consumes the information. Only limited data is sent to the cloud server that is needed for critical and sensitive processing. Due to the limited data transfer, the bandwidth utilization of the network is optimized improving the network latency and response time.

2) *Components*

a) *Edge Device:* Edge devices have more capabilities than the IoT device in a way that they are capable of storing and processing the captured data locally.

b) *Edge Server*: Edge servers are the general-purpose racked computers that are capable of interacting with the IoT/Edge devices by using agents. [1] They are usually located at the same facility where the end devices are.

c) *Edge Agent:* Edge agents are installed on each of the edge devices. It is the middleman between the edge device and the edge server.

d) *Central Cloud Server:* This is the enterprise cloud server where the complex and sensitive data processing takes place. It is usually situated miles away than the end device.

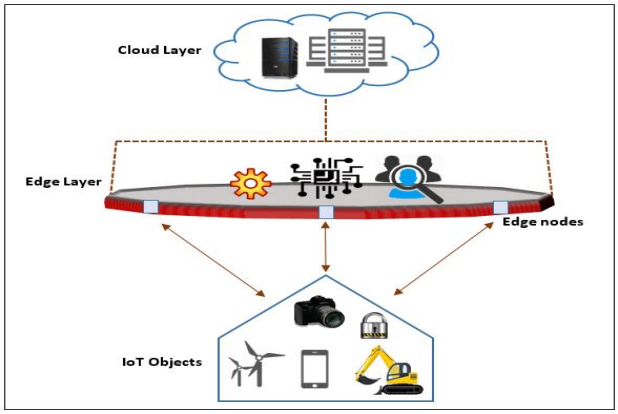


Fig. 2 Edge computing topology

3) Working of Edge Computing

The edge device captures the raw data with the help of sensors.

a) This captured data is processed by the edge device itself locally.

b) In case the device is not capable of handling the data, it sends this data to the edge server via edge agents.

c) Edge servers stores and processes the data locally and sends only the critical or sensitive information to the centralized cloud server.

d) The cloud server upon receiving the information from either edge device or edge server performs the optimum computing and data storage.

In reference to the section#2.1.3 "Working of IoT": case#2, where the facial recognition algorithm is invoked through a cloud-based service to validate with the access management data stored on the cloud. This would take a lot of time to process. With an edge computing model, the algorithm could run on an edge device or edge server locally given the increasing power and storage capabilities on the device while sending limited information (like access time, Person ID etc.) to the cloud.

The major drawback of such systems is security. Since the critical and sensitive information is either stored at the local edge device/server or the centralized cloud server, it is more prone to security threats and data breach. Chances are that the facial recognition details could be altered by any hacker who manages to gain the access to the edge device/server or cloud server. With the implementation of blockchain technology this risk could be eliminated entirely. Blockchain transforms the way data is being handled, processed, and delivered in the distributed system. In the following section, we will discuss how blockchain helps to build a tamper proof system.

C. Blockchain

1) Description: Blockchain is decentralized, publicly available ledger that stores the transactional information distributed over the network in the form of blocks. Each of these blocks are interlinked to previous block in the chronological order. The data in the block is available to everyone but is immutable. The hashing mechanism ensures the data integrity. Every block has a unique hash of its own and the hash of the previous block. Whenever a transaction is initiated, the new block is verified by all the nodes of the blockchain. Once it is verified, this new block is always added to the end of the blockchain. [2] The size of the blockchain keeps growing based on the amount of transactions committed. This may be a potential performance bottleneck over the time. Also, increase in memory under-load indicates a possible increase in block data limits or maximum transaction complexity. [3]

2) Components

a) Node: user or computer within the blockchain architecture that consists of copy of the entire blockchain ledger (publicly available)

b) Block: a data structure which holds all transaction details, a timestamp and cryptographic hash of the previous block

c) Chain: a sequence of blocks in a chronological order

d) Transaction: smallest building block of a blockchain system that is used to transfer the cryptographic data (records, information, etc.) in the form of blocks

e) Miners: participating nodes who solves mathematical problems to validate the transaction and add it to the public ledger [4]

f) Consensus (Algorithm): mutually agreed set of rules to derive a single data value in a distributed system. This generates trust and reliability among the miners [5]

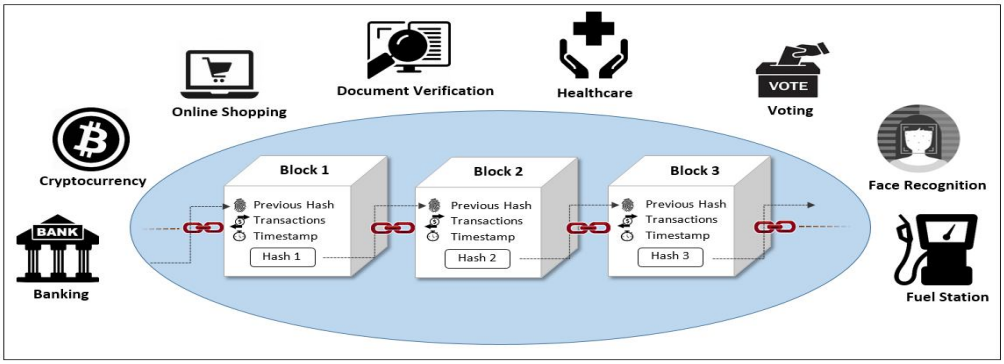


Fig. 3 Blockchain Network

3) Working of Blockchain

a) When a transaction is initiated, all the miners in the blockchain network are notified.

b) These miners compete with each other to validate the transaction by solving a mathematical problem or Proof of Work(PoW)

c) Once the transaction is validated by a specific miner, the block is generated containing *transactional details, a unique* hash and the timestamp.

d) Once the block is generated, it is added to end of the blockchain and is publicly available.

Whenever someone tries to modify the information in the existing block say 'BlockA', the hash of the block will also get changed. The next block say 'BlockB' will notice the change in the hash of the BlockA as it was recorded by it when the BlockB was introduced to the chain (as each block includes the hash of the previous block). In order to modify a single block i.e. BlockA, the previous hash value in all the successive blocks (BlockB, BlockC, BlockD, and so on) must also be updated. This update has to be much faster before a new block is added to the chain. So, unless you have a powerful computing speed which is more than the aggregated computing speed of all the nodes in the chain, modifying all the successive blocks will be challenging. Moreover, the success of this is not guaranteed due to the consensus protocol of the blockchain. [6] The Consensus will not allow this to happen and flag this modification as unintended one and reject this modified block from the chain. This makes blockchain a **tamper proof** network.

II. THE NEED FOR INTEGRATION

The aforementioned technologies have their own strengths and challenges. However, when they are integrated, they complement each other quite well and boost the capabilities and performance of the overall system. While IoT connects the various segments of the world digitally ensuring high standard of living, it makes human life comfortable and easier through automation. Due to exponential growth in the usage of IoT in the recent years, these devices are compromised on size restricting its computational power and storage limits so as to compete with other market competitors. [7]

Edge computing supports IoT to offload its computational and storage limitations thus improving the network latency and responsiveness of the system. Due to the exposure to the openly coordinated computing environment, it is more susceptible to security threats like *DDoS attacks*[8] wherein multiple computer systems emulating edge server bombard a targeted server with huge number of parallel requests to deny the service to the IoT device and to make it even worse it can break the server. Incorporating blockchain ensures reliability and integrity in the system. Any malicious activities are detected and rejected before it is committed to the blockchain network. Though blockchain provides guarantee on security front, the miners in the blockchain network has stringent requirements on the computational storage and bandwidth needs.

Edge computing complements blockchain by facilitating the data transfer in the distributed network following the blockchain's consensus protocol. This creates a confidential and distributed environment where not only the computational capabilities are offloaded to the edge but also it is highly secured in the distributed environment. [9] It thus becomes a need to integrate these technologies for the effectiveness and sustainability of the high demanding needs of the modern world.

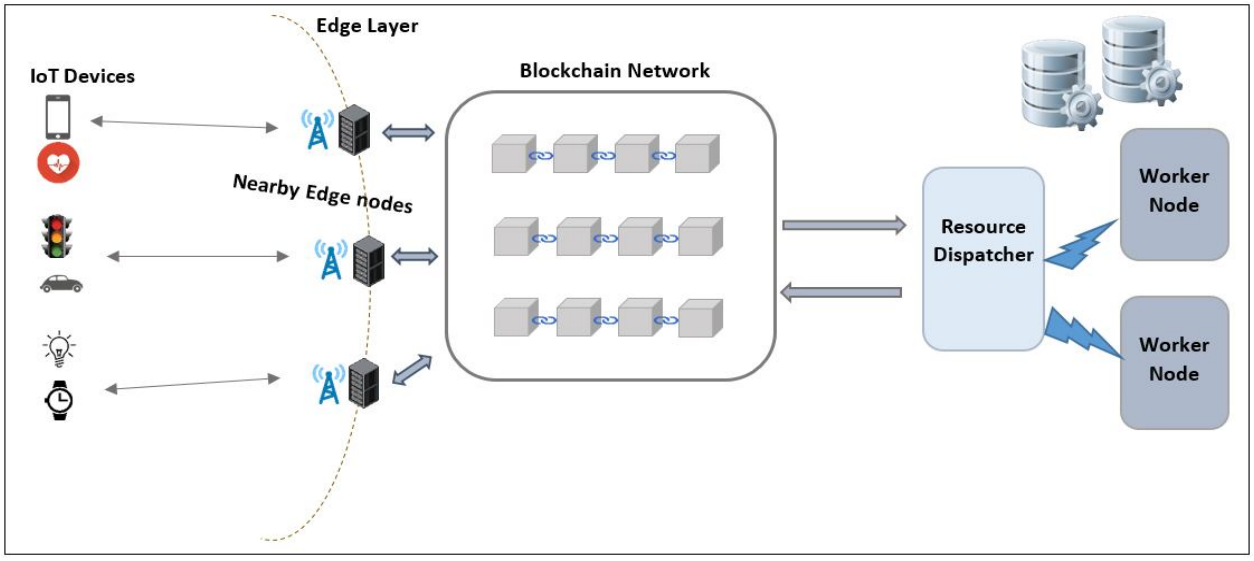


Fig. 4 Pictorial representation of integrated system

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

III. PERFORMANCE TESTING OF INTEGRATED SYSTEM

The performance of the overall system can be measured on various factors such as volume-based evaluation, verification of the application's ability to scale up/down, system behavior under spike. Also, it is much important to performance test the integrated system over various networking conditions to keep the latency at its minimum.

A. Volume Testing

While the IoT technology has the ability to make things smarter, we need to measure its performance as the volume of data collected over the period of time is so huge that it tends to become a potential performance bottleneck. This may gradually lead the IoT objects to respond late. Evaluating the integrated system thoroughly with respect to performance would ensure the success of IoT technology. Also, the edge network should be capable of handling the enormous data during peak hours of usage without breaking the entire system. Being a secure way of data handling, the blockchain technology has been adopted by many applications eventually increasing the load on the system. This causes increase in number of transactions achieved in the network. Hence it is needed to test the blockchain structure against this increasing volume that will ensure the integrity and availability of the data in the integrated system. [10]

B. Scalability Testing

With the increase in the amount of IoT devices being manufactured and used in the various utility sectors, measuring application scalability also becomes a major concern in IoT system as well as Edge computing infrastructure. Over the time, the central system may show the bottleneck in terms of handling maximum concurrent connections and memory usage to support these devices. The server might respond slowly destroying the sense of existence of the IoT technology. Moreover, the micro data centers located at the edge might also break the system and hence should be capable of auto-scaling. With the increase in number of transactions, blockchain keeps on growing in size by adding new blocks in the chain and hence its performance effects on overall system must be measured. [10]

C. Spike Testing

This testing becomes necessary to identify the application's ability to recover under extreme load conditions. Considering the rapid growth in the adoption of IoT, Edge Computing and Blockchain, spike testing with the unexpected rise and fall in the load must be done. A proper analysis of the application usage, peak hour time and network conditions is needed. For example: In the controlled environment, network outage condition can be simulated wherein users are unable to do any transactions with the help of IoT device causing less load on the overall integrated system. Performance of the overall system can be measured against several metrics at this point. When the network outage condition is resolved and internet connectivity is restored, users will shoot up the load on the system. Here we can again measure system's performance under this extreme spike condition. System will take some time to stabilize and recover but that time should be as low as possible. Various other testing can also be preferred like **Soak test** where the system is allowed to be utilized for a longer duration under normal load conditions. Performance issues like memory leak can be identified as the outcome of this test. Also, to identify the breakpoint of the overall system, **Stress test** can be performed by simulating gradual load for a specified duration and observe various metrics for system's performance.

IV. KEY SERVICE LEVEL INDICATORS

A. Throughput

Achieving maximum throughput is the core requirement in the shared network having limited resources with millions of devices. The edge servers must share the information which is really needed for cloud computing to achieve maximum throughput. However, it also depends upon block size. Ideally the block size is directly proportional to throughput of the system.

B. Network Latency

It is the amount of time taken by the source system to send the data to cloud servers. It is important to drill down latency at each component level. Network latency is directly proportional to the block interval, hence it should be measured and monitored with various block intervals. Note: Higher block interval may make system unstable.

C. Transactions Per Second

Having confidence on the rate at which transactions can be processed in a second is beneficial in blockchain and edge computing enabled IoT systems. An agreeable balance between throughput and network latency has the ability to amplify the transactions achieved per second. [11]

D. Response Time

Measure the response times from all the interfaces i.e. IoT-Edge & IoT-Edge-Blockchain to be able to identify that component of the architecture which could be the potential performance bottleneck of the integrated system. This ensures that system's integrity is maintained under typical load conditions. Also be aware that higher the block size, higher would be the block verification and propagation time. Hence block size needs to be set to an optimum size that justifies the response time.

E. Memory Utilization

Memory is the supreme need of such a complex solution. The cloud server could be overloaded with the increased number of incoming messages from the integrated system which may result into high memory consumption. Memory utilization is directly proportional to block size and transaction complexity. The block size must be defined such that it doesn't exceed the memory utilization threshold. Issues like memory leakage could be identified through soak testing. [3]

F. CPU Utilization

The CPU utilization must be monitored for Blockchain and Edge separately as the edge servers are offloading most of the computational tasks while blockchain does the transaction processing. There is a huge computational requirement from the blockchain network to solve the PoW based on a complicated consensus. Increased amount of transaction which are more complex may lead to high CPU requirement. While drilling down the cause for high CPU, metrics like System time, user time and IO wait time shall be accounted. [3]

The above SLIs must be accompanied with the predefined Service Level Objectives (SLO). Having detailed questionnaire session with the stakeholders will help to define the threshold values of the above SLIs. It is not possible to cover all the performance counters in the scope of this white paper. Other counters should be also be considered while garnering the goal of the performance testing.

V. TEST APPROACH

Having a well-planned approach to test such complex applications is very important. If the approach is correct then the entire performance testing efforts (time, Money, investment) will yield maximum benefits in terms of detecting the bottlenecks in your application. Below are the factors that will help you to build a meaningful test approach.

A. Test Environment Setup

A mock system needs to be setup that will simulate the IoT device behavior and blockchain functionalities.

Identify custom IoT-Data endpoint for communication, define rules for data processing and integration with edge servers, setup log level appropriately. [12] The resource lenders and worker nodes are needed for processing the transaction requested by IoT device. Blockchain and IoT usecases can be simulated using the API/Plugin. Also, the testing infrastructure to be setup based the traffic observed in the production. To simulate millions of IoT devices, there will be a need of multiple and powerful load injectors.

B. Scripting Approach

It starts by ensuring that appropriate protocol has been selected. Make sure that the API libraries are imported to the scripting workspace. Start building the script step by step by subscribing to the API functions, like for IoT an API publishing the events just like a payload message resembling the sensor data, API to push this data to the Edge server's endpoint for on premise processing. Another set of APIs for simulating blockchain's functionalities can be used. For example ChainEndpoint to get the blockchain details about its height, timestamp/hash of the latest block, and number of transactions, WalletAPI to group multiple public addresses under a single name, transaction API to lookup information about pending transactions, query transactions based on hash, create and propagate your own transaction and embed data on the blockchain.[13]

C. Workload Simulation

The objective behind the performance testing must be defined clearly so as to simulate the workload accordingly. Even though the overall system is complicated in nature, the production like load simulation is a must criterion. Production logs or pre-existing database benchmarks can be analyzed to understand the expected load pattern required to be performance tested. As mentioned in the section#4, a particular performance test type or combination of few of them can be executed based on the business needs. Every test executed can be scored based on SLI and defined SLO to determine the success factor of the test.

VI. CHALLENGES FACED DURING IMPLEMENTATION

A. *Testing Tool and Protocol Selection*

1) *Problem:* Since IoT system uses custom/non-standard protocols like MQTT, CoAP, AMQP, XMPP, DDS, and REST APIs over HTTP etc., implementing the usecases with a proper tool and protocol selection becomes a major challenge for IoT and blockchain both.
2) *Solution*: A proper tool analysis needs to be done as per the protocol that suits well to the application under test before finalizing it. [14] Also, since blockchain APIs are less user friendly, we need to gain more insights into scripting and testing the blockchain application. Using a performance test tool that supports the SDK and required libraries would be breakthrough however supporting plugins from technology vendors may also help significantly.

B. *Test Environment Setup*

1) *Problem:* Setting up the testing environment as close as possible that resembles the production environment is very critical. A considerable deviation from the test environment configuration may lead to unreliable test metrics. Also, a low configuration test bed may be a roadblock to the testing infrastructure.
2) *Solution:* A good test architecture stack enables the replication of potential performance bottlenecks. Blockchain requires high computational power for transaction processing hence using high end load generators machines may contribute significantly to simulate the real-time load and support the testing activities up to a great extent.

C. *Realistic Load Simulation*

1) *Problem:* With the exponential growth in the acceptance of IoT technology, we might end up using millions of devices for real time load simulation. This is practically impossible and also need great investment, causing the constraint on replicating real time load on IoT systems.
2) *Solution:* The IoT devices can be simulated through virtual users from any performance testing tool preferably cloud based for example Neoload Web, Load Runner Cloud, etc. Additionally, refer the IoT API documentation for simulating the expected behavior of the device when the testing tool is integrated with the IoT plugin for usecase simulation. User load patterns must also be aligned with the actual usages and the respective non-functional performance benchmarks and expectations.

D. *Geographical and Network Simulation*

1) *Problem:* The IoT objects may be geographically distributed several miles away and the time to respond proportionate directly to the latency observed in the network. Also these devices are operating under different networking conditions. It becomes challenging to simulate such user population from any regular performance testing tool. [15]
2) *Solution:* Cloud based testing platform provisions the usage of load injectors that could be located across multiple geographically situated data centers. It helps to determine the network latency patterns effectively.

E. *Data Consistency*

1) *Problem:* As we are dealing with distributed testing components, having a consistency in the data structure becomes a major challenge to achieve. Since the blockchain transactions are irrevocable, we must ensure proper handling of blockchain and their transactions while testing under stipulated load.
2) *Solution:* Having periodic and controlled housekeeping jobs automated (possibly through a defined CRON expression) can help to achieve data consistency. A rollback recovery mechanism can also help to achieve the stability by saving the state of the stable version of data structure through a checkpoint. It can then be rolled back to the checkpointed state over a period of time or post the set of test executions.

VII. DRAWBACK OF INTEGRATED SYSTEM

Though the components of this architecture complement each other quite well, but still there is one major drawback which could bring down the success of this integrated implementation and that is "*Scalability*". Such issues are observed with growing usage of IoT devices and the way how blockchain operates. Each and every transactions and block information are stored on every node in the network permanently. The demand for storage, network bandwidth and computation power eventually increase with the expansion of the network. Moreover, the manufacturers have been compromising on the computation and storage capabilities of these devices with the competitive market. This creates a major impediment for attaining maximum throughput while keeping the network latency to its minimum [9].

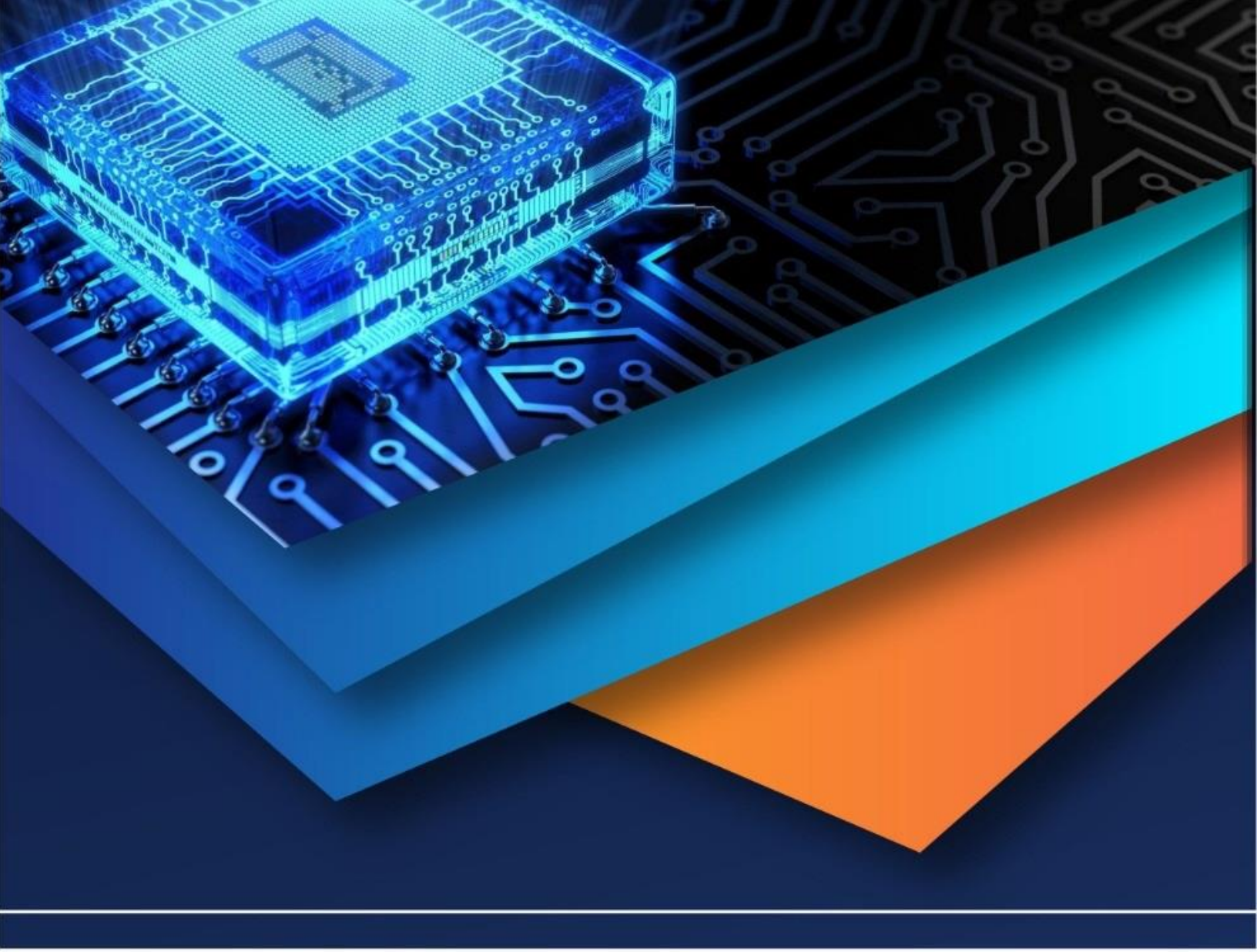
One of the suggested ways to overcome scalability issue is to store data into the side chain. As soon as the transactional data moves to the side chain, the block becomes free to store future transactional data. This technique is called as "*Softfork*". [16]

VIII. CONCLUSION

The objective of this literature is to achieve a highly performing design of IoT by integrating two highly trending technologies, blockchain and edge computing. These technologies have emerged in this decade and there is limited awareness on the topic. Investing sufficient time on having a good test approach and orchestrating production-like test environment based on the needs of the business critical and compute-memory intensive tasks becomes the necessity for the success of the testing activities. Simulating realistic load and tailoring key metrics as stated in the section#4 will help pinpointing the potential SUT bottlenecks with minimum test execution cycle. Despite of the aforementioned scalability issue, this integrated system provides various advantages which cannot be overlooked. Identifying scalability issues and addressing them effectively before time can grow the business of IoT exponentially as forecasted by Gartner in its press release August 2019. [17]

REFERENCES

[1] Iyengar. (2019) Architecting at the Edge. [Online]. Available: https://www.ibm.com/cloud/blog/architecting-at-the-edge
[2] A. Rosic. (2016) What is Blockchain Technology? A Step-by-Step Guide For Beginners. [Online]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology/
[3] B. Wooger. (2019) The Key Metrics to Measure Blockchain Network Performance. [Online]. Available: https://hackernoon.com/how-to-measure-blockchain-network-performance-key-metrics-en1234u4
[4] D. Cosset. (2018) Blockchain: What is Mining?. [Online]. Available: https://dev.to/damcosset/blockchain-what-is-mining-2eod#:~:text=Miners%20validate%20new%20transactions%20and,the%20Proof%2DOf%2DWork.
[5] M. Rouse, M. Haughn. (2017) Consensus Algorithm. [Online]. Available: https://whatis.techtarget.com/definition/consensus-algorithm
[6] M. Orcutt. (2018) How secure is blockchain really?. [Online]. Available: https://www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/
[7] A. Borodinets. (2019) IoT Performance Testing — In Search for Weak Spots. [Online]. Available: https://medium.com/iot-why-not/iot-performance-testing-in-search-for-weak-spots-d7abd6161b30
[8] Dr. O. Baecker, S. Jain. (2020) Can blockchain accelerate Internet of Things (IoT) adoption?. [Online]. Available: https://www2.deloitte.com/ch/en/pages/innovation/articles/blockchain-accelerate-iot-adoption.html
[9] B. W. Nyamtiga, J. C. S. Sicato, S. Rathore, Y. Sung and J. H. Park, "Blockchain-Based Secure Storage Management with Edge Computing for IoT" in *MDPI, Electronics 2019*, vol.8 (Issue 8), page 828, [Online]. Available: https://www.mdpi.com/2079-9292/8/8/828
[10] (2019) Smartsourcing Global, Inc website. [Online]. Available: https://www.smartsourcingglobal.com/blockchain-testing-2/
[11] I. Eyal, A. E. Gencer, E. G. Sirer, and R. V. Renesse, *Bitcoin-NG: A Scalable Blockchain Protocol*, in Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI '16), 2016, page 45-59. [Online]. Available: https://www.usenix.org/system/files/conference/nsdi16/nsdi16-paper-eyal.pdf
[12] (2020) Amazon Web Services, Inc website. [Online]. Available: https://docs.aws.amazon.com/iot/latest/apireference/Welcome.html
[13] (2020) BlockCypher Website. [Online]. Available: https://www.blockcypher.com/dev/bitcoin/#blockchain-api
[14] (2017) QA EliteSouls LLC Website. [Online]. Available: http://www.qaelitesouls.com/2017/03/22/iot-performance-testing-challenges/
[15] Y.R.Gurijala. (2018) Performance Testing Internet of Things (IoT). [Online]. Available: https://www.infosys.com/de/documents/performance-testing-iot.pdf
[16] I. Pavlenko. (2018) Blockchain Scalability: Hard Forks, Lighting Network, and Plasma Cash. [Online]. Available: https://applicature.com/blog/blockchain-technology/blockchain-scalability
[17] L. Goasduff. (2019) Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io#:~:text=Gartner%2C%20Inc.,a%2021%25%20increase%20from%202019.&text=Utilities%20will%20be%20the%20highest,to%20reach%201.37%20billion%20endpoints



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY