[*1]Nuras Naser Saeed Hizam,

[2]Madhukar Shelar,

[3]Archana Bachhav

Internet of Things and Diversity of Device's Frameworks and Architectures: Survey

Abstract: - People are enamoured with the Cryptocurrencies Bitcoin and Ethereum, which have recently gained enormous popularity. The success of various Cryptocurrencies is due to blockchain. Every sector is aware of and using the advantages of blockchain. Because of the daily expansion of the technological revolution, practically everything is now done digitally. As a result, security, the most important factor, is required. Blockchain acts as a super hero by offering a protected conduit for transactions. It is a chain of blocks, as the name would imply. Digital data is referred to as a block, and the public database is referred to as a chain. It is utilized in supply chains, healthcare, property records, and other areas. The purpose of this paper to expose the implementation of the blockchain in IoT Platforms and provides an in-depth analysis of several categories of consensus protocols implemented in different blockchain systems, as well as the advantages and disadvantages of every algorithm. We additionally present an underlying comparison of several algorithms to help in better comprehend consensus protocol choosing. We elicit the IoT issues being taken into account as well as the specifics of the blockchain-based solutions.

Keywords: Cryptocurrencies, Bitcoin, Ethereum , Block chain, consensus algorithms, IoT.

I. INTRODUCTION

The Internet of Things (IoT) intends to create intelligent environments by connecting physical objects to the internet and sharing data in a peer-to-peer manner [1]. In areas including the energy grid, manufacturing, and supply chain, business projects have been developing IoT platforms. Developers, however, have difficulties in the creation and administration of IoT platforms [2]. An IoT platform consists of a large number of Things, and typically, a central node controls every linked Thing. Single points of failure are introduced by a centralised architecture like this. Second, it is inefficient for centralized servers to manage all the data gathered by Things in the IoT platform since it necessitates extensive processing resources [3], [4]. Thirdly, managing Things is challenging since there isn't a set standard for doing so. This is because managing Things doesn't handle concerns like data privacy, data security, thing security, and system upkeep for a large number of connected Things [5]. A
blockchain is an immutable distributed ledger that is kept up-to-date by a peer-to-peer network, where the participants must agree on the statuses of transactions uploaded to the blockchain network in order for the transactions to be legitimate [6]. No centralized, reliable third party is required for the blockchain network to function. Additionally, every member of a blockchain network has a local copy of every transaction that has

[1*]Ph.D. Scholar
CMCS College, Nashik
Savitribai Phule Pune University
Pune City, Maharashtra State, India
Naser.nuras@yahoo.com
[2]MVP Samaj's Commerce Management
and Computer Science, Nashik
Savitribai Phule Pune University
Pune City, Maharashtra State, India
mnshelar70@gmail.com
[3]MVP Samaj's KSKW Arts, Science
and Commerce College, Nashik
Savitribai Phule Pune University
Pune City, Maharashtra State, India
77.archana@gmail.com

ever taken place. This guarantees the system's high availability and gives network members access to transparent data. Researchers are looking at the possibility of utilizing blockchain to address current IoT difficulties because of the decentralized structure of blockchain and the distinctive qualities it offers [7]. The majority of the current efforts in this field, however, either concentrate on the conceptual level or are still in the very early stages of merging two technologies.

II. OVERVIEW OF BLOCKCHAIN

The world's most important unit is data. Data storage, processing, and analysis are challenging task, and new technologies are emerging to make them as simple as possible. Hackers can access the data since it is centralized. Decentralized cloud data is however required. Cloud storage is the popular technique of data archiving. It is in high demand and frequently mishandled as a result. All of the information is centralized, which is the major limitation. Transactions make the data insecure and unsafe since it is typically not encrypted. Decentralized cloud data is more secure and makes it more difficult to hack. It also lowers the price.

II.I The Use of Blockchain Capabilities for storage in IoT

Using blockchain, there are two approaches for storing data: on-chain and off-chain. As the name implies, all the data is saved on the chain in an on-chain manner within each block. As a result, in the event of an assault, data can be recovered and utilized. This is an expensive Endeavour, but everything has a price. Due to network and data saturation, it occasionally even costs a lot. As a result, off-chain storage is frequently employed. Off-chain storage just stores the metadata and not the actual data. But there is a drawback. The data might not be restored if there is a system breach. Nevertheless, they are inexpensive, which makes it the ideal choice.

II.II IoT Related Blockchain Features

Both technologies (IoT and Blockchain) have various benefits that may be combined to provide better results. Adopting a decentralized strategy of the block-chain for the IoT will address numerous challenges, including security, and the technology offers limitless possibilities. Adopting the standardized peer-to-peer communication model to handle the hundreds of billions of device-to-device transactions will significantly lower the costs associated with setting up and maintaining large centralized data centers and will distribute computation and storage needs across the trillions of devices that make up IoT networks. This will stop a network from collapsing completely if just one node in the network fails [8]. The below table shows variation between block chain and IoT.

Table 1. Variation between IoT and Blockchain

	IoT Technology	Blockchain Technology
1	Centralized	Decentralized
2	Requires Low Latency	Time-Consuming for Block Mining.
3	Devices in the Internet of Things are Expected to be Vast.	Scalability with Vast network is Low
4	IoT Devices Have Constrained Bandwidth and Resources.	Excessive Bandwidth Usage
5	One of the Major Challenges with IoT is Security.	Recently Has developed Security
6	Limited by Resources	Consuming Resources

The blockchain is the ideal component to become the core of IoT solutions because of its decentralized, autonomous, and trust less properties. It is not surprising that enterprise IoT technologies are among the first to use blockchain technology. Yet, developing peer-to-peer interactions will have its own set of challenges, particularly in terms of security. IoT security considers more than just securing private Sensitive information. Hence, in order to combat fraud and theft in IoT networks, blockchain solutions will need to retain privacy and security and employ participant validation and approval for transactions [9].

Moreover, blockchain technology is seen as one of the primary answers to the IoT's privacy and dependability p roblems. It may be used to monitor billions of linked devices, enabling the processing of transactions and coordi nation amongst devices, allowing for considerable cost reductions for IoT sector manufacturers[10].This

decentralised strategy would also do rid of single points of failure, making the platform on which devices functi on moredurable. As blockchains employ cryptographic methods, customer data would be more secure [11].
The integration of blockchain and IoT has been found in many studies which reviewed the state of art of blockchain and IoT. While some articles described blockchain as a holistic solution, many studies concentrated on only two aspects of the technology: smart contracts and consensus protocols. There are several additional papers that are primarily concerned with the use cases, as well as those that are mostly concerned with the security characteristics of the solutions. In accordance with their areas of emphasis, these relevant security studies are categorized into two categories:

III. Smart contracts.
IV. Consensus algorithm.
IV.I. PoW (Proof of Work)
IV.II. PoS (Proof of Stake)
IV.III. PBFT(Practical Byzantine Fault Tolerance)
IV.IV. DPoS (Delegate Proof of Stake)

III. SMART CONTRACTS

The concepts of smart contracts are discussed in the article of Lucci, N., & Ketel, M. [12] they stated that Smart contracts are scripts that are integrated into the Blockchain system and are designed to run specific external functions after a successful network transaction. Smart contracts are advantageous because they enable general-purpose computations and automation to work alongside the Blockchain. The Author outlined implementations of smart contract in (smart house scenario) and their related benefits and drawback. The Author stated that three threats prevent user from accessing services and implemented the use of smart contract for blockchain to counter these issues and improve the performance of the smart house devices. As well Christidis and Devetsikiotis [13] focused on smart contracts and claimed that the combination of smart contracts and IoT technology may introduce new business models to the existing systems and enhance present working procedures, they discussed the result of blockchain network functions and how smart contracts could improve the manner in which that interactions between parties dealt in transactions on a network could be managed and performed out automatically. In project which is named FairAccess [14] which is uses blockchain-based smart contracts to exchange access tokens for the fulfillment of access control regulations. The Author proposed security and privacy-preserving objectives for analyzing privacy and security in IoT, he stated that the use of the smart contract enabled their framework to express fine-grained context aware access control policies. The proposed framework tried to leverage the consistency offered by blockchain-based Cryptocurrencies such as Bitcoin to provide a stronger and transparent access control tool. Bagchi explores the potential of blockchain and smart contract to access management of IoT in her master thesis [15]. With the help of the Ethereum blockchain, a proof-of-concept and model for a more straightforward access control mechanism were developed. So far, a client access request has just led to the development of an access rule, which has been uploaded to the blockchain network. In the other hand Zhang et. al.[16] presented IoT access control system based on smart contracts. The system employs three different types of smart contracts: access control contract (ACC), judge contract (JC), and register contract (RC). Access control policies, such as resource and permission pairs, are contained in ACC. For those subjects that misbehave, JC uses a misbehaviour-judging system and applies the appropriate sanctions. Last but not least, RC oversees the mechanisms for misbehaviour-judging and access control (in ACC) (in JC). Blockchain is not completely utilized in the IoT system design, for example, a centralized storage device is still employed. Lin, Chao, et al.[17] in their paper built a secure mutual authentication system, Particularly the suggested system integrates blockchain, group signature, and message authentication code in order to offer accurate monitoring of user access history, anonymously authenticate group members, and effectively authenticate home gateway, which could be utilized by smart home applications. as demonstrated results The suggested system utilized a Group Signature and Message Authentication Codes to authenticate a requestor without disclosing information about the particular user or the home gateway, accordingly, with complete forward secrecy. The use of blockchain smart contracts for offering security services in the Internet of Things and other connected devices was thoroughly reviewed in the literature review paper , which was provided by Lone, A. H.[18] et al. the paper showed that access control, authentication, integrity assurance, data protection, secure key management, and non-repudiation are the most frequently used smart contract-driven security services. the paper also demonstrated that Hyperledger Fabric and Ethereum were the two most popular Blockchain platforms for creating security solutions based on smart contracts.

IV. CONSENSUS ALGORITHM

With immutability, privacy, security, and transparency, blockchain is a distributed, decentralized network. Despite the absence of a central authority to validate and verify the transactions, the Blockchain is thought to have a perfect security and verification system in place for all transactions. Just because the consensus mechanism, a fundamental component of every Blockchain network, is there is such a thing conceivable. The Blockchain network's peers use a consensus method to come to an understanding about the current state of the distributed ledger. Consensus algorithms enable dependability in the Blockchain network and create authority amongst insecure peers in a distributed computing environment in this way. In essence, the consensus protocol ensures that each new block added to the Blockchain follows a certain set of rules. Therefore, a consensus algorithm seeks to establish an approval that benefits the entire network. Therefore the blockchain uses a few several consensus algorithms such as like , A. PoW (Proof of Work) , PoS(Proof of Stake), DPoS(Delegated Proof of Stake), PBFT(Byzantine Fault Tolerance)

IV.I. PoW (Proof of Work)

The initial consensus technique in a blockchain network is called Proof of Work (PoW). Proof of work supports secure peer-to-peer transaction processing without the necessity of trusted third party. The algorithm adds a new block to the chain and confirms the transaction. In this method, minors (a group of individuals) interact with one another to finish the network transaction. Mining is the activity of interacting with one another. It gets a reward as soon as miners have successfully produced a valid block. Bitcoin is the most well-known Proof of Work (PoW) application. many various studies developed blockchain solutions that use proof of work starting with S Algarni et al [19]. In order to manage the supply of lightweight and decentralized safe access management of an IoT system, this paper provides a unique method based on a multi-agent system and a blockchain. Building Blockchain Managers (BCMs) for protecting IoT access control and enabling secure communication between local IoT devices is the major goal of the proposed approach which implemented using Proof of Work (PoW). Additionally, the approach allows secure interactions between cloud computing, fog nodes, and IoT devices. C. Gupta and A. Mahajan [20] presented the principles of blockchain technology, the construction of the Proof-of-Work consensus algorithm, and a study of its performance. The paper addresses the fundamentals of blockchain technology and reviews the effectiveness of the PoW algorithm based on various degrees of mining speed and difficulty. Depending on the needs of the organization, security or speed might turn out to be higher priorities. Furthermore, results of the paper show that the PoW algorithm requires machines with enormous GPU power, which raises the cost and utilize a lot of energy. As thus, using ordinary machines for the purpose of mining is not at all advised. The PoW algorithm also has other disadvantages, including the fact that it requires normal machines to take several hours or even days to mine a single block. Because of this, the PoW method is not advised for organizations where resources have limitations and time is a concern.

IV.I. PoS (Proof of Stake)

Cryptocurrencies require a method of transaction verification since they are decentralized and independent of financial institutions. Proof of stake (PoS) is one technique that many cryptos utilized. Cryptocurrencies operations are verified via a form of consensus process called proof of stake. With this mechanism, cryptocurrency holders can stake their coins, giving them the authority to review and add new blocks of operations to the blockchain. This approach is the substitute to proof of work, the first consensus mechanism introduced for Cryptocurrencies. Proof of stake has grown in popularity as concern about the environmental impact of cryptocurrency mining has increased since it is significantly more energy-efficient. A study of Samaniego, M. et al [21]. Used the concept of PoS consensus, In order to improve IoT services on edge hosts, this study investigates the idea of merging a permission-based blockchain for virtual resources. As well as Niya, S. R. [22] in study used a PoS in blockchain for IoT. The primary purpose of this study is to present a Blockchain design for IoT data streams. For this reason, a basic Proof of Stake PoS-based Blockchain is implemented, and as direct results, its performance and scalability are increased in order to satisfy the expectations of Blockchain IoT integrated systems. The study also includes the development and execution of an adaption layer for IoT data streams. The developed architecture may handle a variety of hardware and software platforms, as well as network technologies.

IV.I. PBFT(Practical Byzantine Fault Tolerance)

Byzantine Fault Tolerance (BFT) is a distributed network characteristic that allows consensus to be reached (agreement on the same value) regardless of whether some network nodes are unavailable or provide inaccurate information. A BFT method seeks to protect against failures in the system by utilizing group decision-making (both right and faulty nodes) and reducing the effect of the faulty nodes on the network. Failure nodes are classified into two types: crash fault nodes and Byzantine fault nodes. Crash fault nodes fail just by stopping;

thus, nodes simply cease operating with no other destructive behaviours. Messages may only be delaying or missed in this situation. By comparison, Byzantine fault nodes act randomly. They might transmit incorrect messages to other nodes or send various messages to various nodes in order to sabotage the procedure of reaching a consensus. the abbreviation of BFT has come originally from Byzantine Generals' Problem. Many several studies implemented based blockchain using BFT consensus among these studies, Xu, R. et al [23] The primary emphasis of this article is BFT consensus which could emphasis false frame detection using blockchain technology. Edge nodes provide an online based false frame identification as part of the false frame detection process, and they also identify fingerprints of frames via operations that are stored in the distributed ledger. The blockchain network's users can access those fingerprints that have been stored on an unchangeable distributed ledger. As a result, throughout the decision-making process, fog nodes or suppliers of surveillance visualization services can confirm those checkpoint frames. In another paper which examines the possibility of utilizing blockchain technology in order to secure the data of constrained IoT devices which presented by Meshcheryakov, Y., et al. [24], presents the use of the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm to be operated on those devices, and simulates the main distributed records scenarios using PBFT. The study examined typical IoT network situations which could impact system efficiency. They created a simulation tool and executed a series of computational procedures to assess the efficiency of PBFT in common IoT settings. They explored the relationship between the total number of performed blocks and the block size, data production time, and incoming data packet processing delay. They evaluated the highest possible number of devices in a PBFT-based blockchain system based on simulation findings. as a result of this study consensus technique achieves good performance in networks with up to 70 nodes. PBFT may be used to a wide range of IoT systems. In another paper made by Xu, G. et al. [25] The study offers SG-PBFT, a safe and highly effective PBFT consensus method for the Internet of Vehicles based on a distributed blockchain topology. The distributed topology may decrease load on the central server and lower the possibility of single-node assaults. The SG-PBFT consensus method improves on the classic PBFT consensus algorithm by employing a score grouping technique to obtain improved consensus efficiency. The experimental outcomes suggest that the strategy may significantly enhance consensus efficiency and prevent single-node assaults. When the total amount of consensus nodes exceeds 1000. Mišić, J. et al. [26] provided a PBFT ordering service appropriate for addressing specific geographical locations by connecting to proxies that gather data from IoT domains . The consensus method assures that orders in memory pools have the same set of transactions in order that they could be recorded in a blockchain ledger. The service allows ordering inquiries to be processed by any ordering peer, reducing performance penalties and avoiding the single point of failure found in previous PBFT implementations.

IV.I. DPoS (Delegate Proof of Stake)

Delegated Proof Of Stake (DPoS) is a consensus technique that advances the core concepts of Proof Of Stake. Daniel Larimer, founder of BitShares, Steemit, and EOS, created the Delegated Proof of Stake (DPoS) consensus mechanism in 2014. DPoS is being brought up as a beneath consensus mechanism that outperforms its competitors, such as PoW and PoS, by adopting a block production technique that results in more rapid transactions. DPoS saves energy by integrating a one vote per share technique that increases the quantity of processing coins. Liu, W. et al. [27] In their work, presented the donation tracing blockchain model (DTBM) to use blockchain for decentralization, tracking, and anti-tampering to make the contribution process open and transparent. However, the process of Delegated Proof of Stake (DPoS) consensus mechanism is commonly manipulated by a few nodes in existing blockchain systems. the paper enhanced DPoS consensus method for DTBM to prevent centralization and lower the possibility of malicious nodes being picked. The outcomes demonstrate that the donation procedure is observable and identifiable in DTBM. It also overcomes the problem of centralization and enhances security. L Jiang et al. [28] designed a novel wireless power transfer mechanism, that included a contract theory-based wireless power transfer system and a DPoS-based very light consensus technique To achieve the best quantity of transmitted energy and to address the excessive operational overhead of a blockchain's traditional consensus process. The findings showed that the suggested system enhanced the energy transfer usage significantly.

Comparison of Consensus Algorithms Based Blockchain Technology for IoT

Table 2. Comparisons of Consensus Algorithms

Consensus Algorithm	Blockchain Category	Example of Technology	Programming Language	Energy Saving	Security	Scalability	Efficiency	Interoperability
Proof of Work	Permissioned Public	Bitcoin, Ethereum , Monoxide	GoLanguage, Solidity	Not Saving	High	Low	Low	Low
Proof of Stake	Permissioned Private, Public	Peercoin , Ethereum , QTUM	GoLanguage, Python, C++, Java	Partial Saving	Low	Medium	High	Medium
Delegate Proof of Stake	Permissioned Private, Public	EOS , Bitshares	Ruby, Python, JavaSrcipt	Partial Saving	Low	High	High	Medium
Practical Byzantine Fault Tolerance	Permissioned Private, Public	Hyperledger	GoLanguage, Java	Saving	High	High	High	High

We presented in this paper in Table 2 a comparison of several four primary consensus algorithms which are common algorithms used for the blockchain infrastructure used in IoT. This comparison reviewed of consensus algorithms has been conducted in terms of security, energy saving, blockchain category, platform used, scalability, Interoperability, efficiency and programming language. used. If we look at the comparison deeply we can found that first consensus Proof of Work (PoW) can be secure but this consensus protocol has a less scalability comparing to PoS, DPoS and PBFT, in the other hand PoW has the lowest interoperability comparing to others as it is limited consensus protocol which cannot be adopted to deal with various Blockchain which is the permissioned blockchain, in other hands it has less efficiency. When compared to other consensus algorithms, PoW demands the most computing resources. Nodes have to deal with complicated mathematical issues due to the heavy computing complexity in each node. Because they depend on validation devices to protect the network, PoS and its variants require a smaller amount of processing power which mean it energy saving. In the other hand Proof of Stake (PoS) is more efficiency than PoW but it has problem of security risk as it could be attacked. Currently, scalability is a critical component of blockchain, and PoS has very poor scalability because of its higher level of complexity. PoS features contribute in transactions validation, using less processing power as an outcome, which means it is partially saving energy. PoS is more faster in term of performance than PoW which make it equal as compared to DPoS and PBFT.

Delegate Proof of Stake (DPoS) as PoS is weak in term of security comparing to PoW and PBFT, but it is much more better in energy consumption than whatever in PoW as it is partially saving processing power.
PBFT is an excellent consensus technology; however it is only adequate to permissioned Blockchains. Despite being much faster than other protocols, it is also higher interoperability than PoW, PoS and DPoS, it offers great interoperability since it uses a widely known consensus technique which can be capable to operate with various Blockchains, as well it has high scalability than PoW and PoS as well higher security than whatever in PoS and DPoS .
Because of the processing power required by the node, Proof-of-Work is incompatible for IoT. Gateways having additional computing capability might be capable to connect to the blockchain via Proof-of-Work. Given the properties of IoT, DPoS and PBFT are more appropriate consensus mechanisms.

V. CONCLUSION

Several sectors have used blockchain technology, and more and more academics, experts and Professionals are concentrating on developing applications for blockchain. Safety and confidentiality issues throughout the application deployment procedure are still quite complicated. Developments and enhancements in

methodologies, techniques and researches are intended and planned to solve the problem of electing block producers, allocating block rewards reasonably, and improving efficiency of ensuring privacy and security. This survey paper summarizes the previous studies regarding integration of blockchain and IoT security issues which categorized into two categories: 1. Smart contracts, 2. Consensus algorithm. Endeavoring to associate in the development of the security of blockchain based IoT networks. The study provides A comparison of several consensus methods was offered to acquire information regarding their efficiency, interoperability, and scalability difficulties. The a classification discussion about consensus algorithms enabled us to comprehend their structured applications in IoT, including permissioned and Permissionless Blockchains. an outline for potential blockchain security and privacy enhancements, with the aim of providing a reference for researchers to help them select and design security methods and consensus algorithms in various application scenarios was also discussed in this survey paper, as well as contributing in the evolution of blockchain application implementation. these enhancements designed to address the issue of blockchain producers, blockchain allocation, and consensus effectiveness while guarantee privacy and security

VI. References

[1] Ashton, K. (2009). That 'internet of things' thing. RFID journal, 22(7), 97-114.

[2] Van Kranenburg, R., & Bassi, A. (2012). IoT challenges. Communications in Mobile Computing, 1(1), 9.

[3] Qiu, T., Wang, X., Chen, C., Atiquzzaman, M., & Liu, L. (2018). TMED: A spider-Web-like transmission mechanism for emergency data in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 67(9), 8682-8694.

[4]

[5] Khan, M. S., & Kim, D. (2015). DIY interface for enhanced service customization of remote IoT devices: a CoAP based prototype. International Journal of Distributed Sensor Networks.

[6] Giang, N. K., Ha, M., & Kim, D. (2015, June). Buddy thing: Browsing as a service for the internet of things. In 2015 IEEE International Conference on Services Computing (pp. 122-129). IEEE.

[7] Lee, H., Sin, D., Park, E., Hwang, I., Hong, G., & Shin, D. (2017, January). Open software platform for companion IoT devices. In 2017 IEEE International Conference on Consumer Electronics (ICCE) (pp. 394-395). IEEE.

[8] Kumar, P., & Pati, U. C. (2016, May). IoT based monitoring and control of appliances for smart home. In 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 1145-1150). IEEE.

[9] Pachube—The Internet of Things Real-Time web service and applications. Available online: http://www.appropedia.org/Pachube (accessed on 2 December 2017).

[10] Sen, A., Modekurthy, V. P., Dalvi, R., & Madria, S. (2016, April). A sensor cloud test-bed for multi-model and multi-user sensor applications. In 2016 IEEE wireless communications and networking conference (pp. 1-7). IEEE.

[11] Kang, S., & Chung, K. (2018). IoT framework for interworking and autonomous interaction between heterogeneous IoT platforms. In Smart Computing and Communication: Third International Conference, SmartCom 2018, Tokyo, Japan, December 10–12, 2018, Proceedings 3 (pp. 217-225). Springer International Publishing.

[12] Ullah, I., Sohail Khan, M., & Kim, D. (2018). IoT services and virtual objects management in hyperconnected things network. Mobile Information Systems, 2018.

[13] Kumar, K., Bose, J., & Tripathi, S. (2016, December). A unified web interface for the internet of things. In 2016 IEEE Annual India Conference (INDICON) (pp. 1-6). IEEE.

[14] Bhawiyuga, A., Kartikasari, D. P., Amron, K., Pratama, O. B., & Habibi, M. W. (2019). Architectural design of IoT-cloud computing integration platform. TELKOMNIKA (Telecommunication Computing Electronics and Control), 17(3), 1399-1408.

[15] Kleinfeld, R., Steglich, S., Radziwonowicz, L., & Doukas, C. (2014, October). glue. things: a Mashup Platform for wiring the Internet of Things with the Internet of Services. In Proceedings of the 5th International Workshop on Web of Things (pp. 16-21).

[16] García, C. G., Meana-Llorián, D., García-Díaz, V., Jiménez, A. C., & Anzola, J. P. (2020). Midgar: Creation of a graphic domain-specific language to generate smart objects for Internet of Things scenarios using model-driven engineering. IEEE Access, 8, 141872-141894.

[17] Prehofer, C. (2015, December). Models at REST or modelling RESTful interfaces for the Internet of Things. In 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT) (pp. 251-255). IEEE.

[18] Niknejad, N., Ismail, W., Ghani, I., Nazari, B., & Bahari, M. (2020). Understanding Service-Oriented Architecture (SOA): A systematic literature review and directions for further investigation. Information Systems, 91, 101491.

[19] Gupta, P., Mokal, T. P., Shah, D. D., & Satyanarayana, K. V. V. (2018). Event-driven SOA-based IoT architecture. In International Conference on Intelligent Computing and Applications: ICICA 2016 (pp. 247-258). Springer Singapore.
[20] Avila, K., Sanmartin, P., Jabba, D., & Jimeno, M. (2017). Applications based on service-oriented architecture (SOA) in the field of home healthcare. Sensors, 17(8), 1703.
[21] Irawan, Y., Linarta, A., & Febriani, A. (2021, March). Smart Home Light Based Service Oriented Architecture and IoT. In Journal of Physics: Conference Series (Vol. 1845, No. 1, p. 012070). IOP Publishing.
[22] Mohamed, A. S., & Al-Atroshi, C. (2018). Adaptability of SOA in IoT Services–An Empirical Survey. International Journal of Computer Applications, 975, 8887.
[23] Fielding, R. T. (2000). REST: architectural styles and the design of network-based software architectures. Doctoral dissertation, University of California.
[24] Nastic, S., Sehic, S., Le, D. H., Truong, H. L., & Dustdar, S. (2014, August). Provisioning software-defined IoT cloud systems. In 2014 international conference on future internet of things and cloud (pp. 288-295). IEEE.
[25] Maurya, R., Nambiar, K. A., Babbe, P., Kalokhe, J. P., Ingle, Y. S., & Shaikh, N. F. (2021). Application of Restful APIs in IOT: A Review. Int. J. Res. Appl. Sci. Eng. Technol, 9, 145-151.
[26] Benomar, Z., Longo, F., Merlino, G., & Puliafito, A. (2020, December). Enabling secure RESTful web services in IoT using OpenStack. In 2020 IEEE 17th international conference on mobile ad hoc and sensor systems (MASS) (pp. 410-417). IEEE.
[27] Garg, H., & Dave, M. (2019, April). Securing iot devices and securelyconnecting the dots using rest api and middleware. In 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU) (pp. 1-6). IEEE.