INDIAN JOURNAL OF
ENGINEERING

18(49), 2021

Analyzing frameworks for IoT data storage, representation and analysis: A statistical perspective

Suniti Purbey[1], **Brijesh Khandelwal**[2]

To Cite:
Purbey S, Khandelwal B. Analyzing frameworks for IoT data storage, representation and analysis: A statistical perspective. *Indian Journal of Engineering*, 2021, 18(49), 151-163

Author Affiliation:
[1]PhD Scholar, Amity School of Engineering & Technology, Amity University, Chhattisgarh, Raipur, India; Email: spurbey@rpr.amity.edu
[2]PhD Supervisor, Head- CSE, ASET/ AIIT, Amity University, Chhattisgarh, Raipur, India; Email: bkhandelwal@rpr.amity.edu

Peer-Review History
Received: 23 March 2021
Reviewed & Revised: 24/March/2021 to 28/April /2021
Accepted: 29 April 2021
Published: May 2021

Peer-Review Model
External peer-review was done through double-blind method.

DISCOVERY
SCIENTIFIC SOCIETY

ABSTRACT

Data representation, storage and processing in Internet of Things (IoT) devices must be done such that the network lifetime and the quality of service (QoS) for the network is minimally affected. In order solve this constraint researchers use sleep scheduling, aggregation, effective data representation, pre-processing, and other techniques. Each of these techniques has its own nuances and advantages. Techniques which involve sleep scheduling improve the network lifetime, but reduce other QoS parameters like speed of operation, while techniques involving pre-processing of data guarantees high throughput but increases energy consumption in the network. A statistical survey of these techniques is mentioned in this text. Moreover, this text also recommends a set of approaches that can be applied in order to improve the performance of IoT networks via better data representation, enhanced data storage structures and effective data analysis techniques. Use of Machine learning and blockchain technologies for improving QoS and security performance of the network are also evaluated. Using this text researchers in the IoT domain can evaluate techniques needed for effective IoT network design and improve the QoS parameters of the network.

Keywords: IoT, Storage, Representation, Analysis, Machine Learning.

1. INTRODUCTION

Internet of Things (IoT) devices have gained a lot of popularity in the past decade, owing to the capability of these devices to remotely monitor, control and actuate inaccessible areas. In order to utilize these capabilities with highest possible efficiency the IoT devices must be designed such that they consume minimum power, require smallest possible delay and provide highest possible throughput. A brief outline of these features can be observed from figure 1, wherein it can be observed each IoT device must be smart (must possess data analysis capabilities), communicant, autonomous, reliable, compact, inexpensive and safe. Each of these characteristics require the device design to incorporate specific computational steps directed towards achieving them.

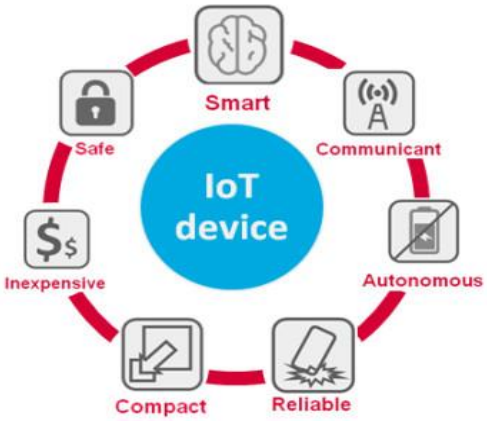

Figure 1. IoT device characteristics

A survey of these computational steps along with their performance measures is showcased in the next section. This allows the readers to evaluate the best combination of techniques that can be used for an optimum system design. Readers can use a hybrid of some of the mentioned techniques for handing application specific issues.

The study will also assist IoT system designers to identify gaps in their existing implementations and find out remedies for the same. This is followed by a statistical analysis of these techniques and some recommendations via which they can be improved. This text concludes with some interesting observations about the reviewed techniques and some further research which can be taken up in this area.

2. LITERATURE REVIEW

Data processing & storage in IoT systems requires a large set of interconnected operations which must be performed in order to improve the data handling capabilities of the device. For instance, a high throughput and low power IoT network must incorporate techniques like data aggregation along with enhanced data communication frameworks. This can be observed from [1] wherein an IoT-based home automation system is described. The system stores sensitive house data using Keccak and chaotic communication schemes. This data-storage framework is deployed on fog-devices, which have high power efficiency and can offload maximum IoT node calculations to improve the device's energy efficiency. The structure for this storage system can be observed in figure 2, wherein the encryption-based computing device is connected between the camera system and the cloud. It can also be observed that the encryption process uses a High Efficiency Video Codec (HEVC) for improving the performance of the underlying system. Due to this, the overall communication error is reduced by 20% thus improving the quality of trans-reception. But the delay of operation for this system is very high. In order to reduce this delay, the work in [2] can be referred. This work divides the input data into hot-data and general data. This division is based on the frequency of data access.

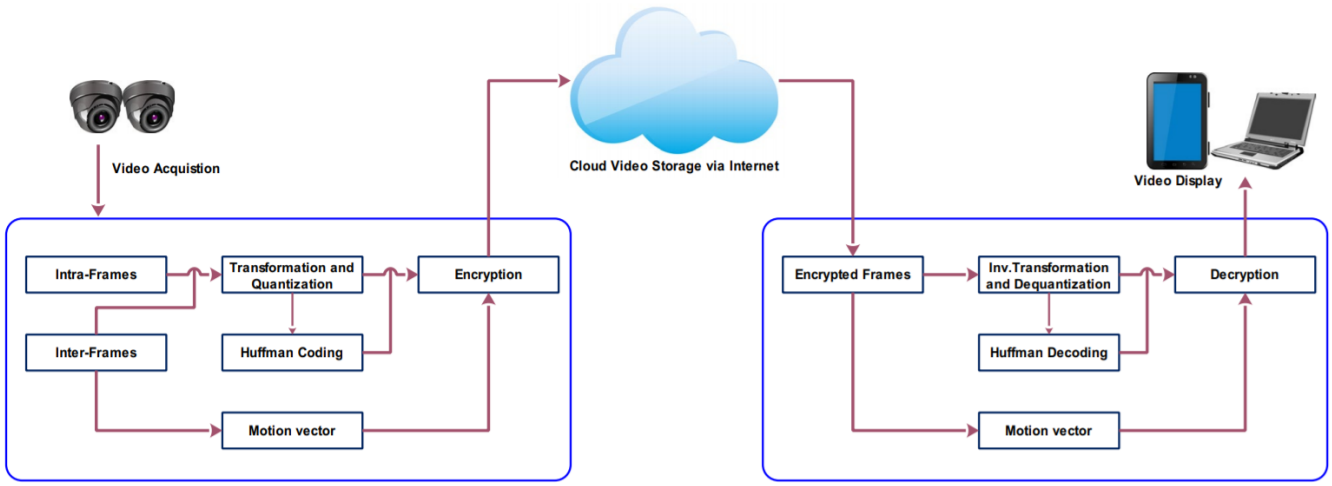

Figure 2. Fog-based encryption for secure IoT

ISSN 2319–7757 EISSN 2319–7765 I OPEN ACCESS

The hot-data is stored in cache memory, and thus is always readily available for access. The general data is stored on normal data memory. Based on the data access patterns, the data is shifted between normal memory and cache memory. On comparison with the PATRICIA-hypercube-tree (PH Tree) method, the proposed algorithm is found to be 20x faster, and thus must be used for real-time purposes. Further comparison of this algorithm can be done with standard algorithms to evaluate its final performance.

Speed of operation and energy efficiency can be further improved using data aggregation and task offloading. This can be observed from [3], wherein a machine learning algorithm is deployed for IoT devices, the algorithm suitably selects which processing tasks must be offloaded to the fog-devices, and which must be performed on the IoT device locally. This distinction is done via a Q-Learning approach, which rewards tasks that are executed on the IoT device under a given set of timing and cost constraints, while it gives a penalty to tasks which do not follow the constraints. Depending upon this reward penalty mechanism the task offloading is done. Data aggregation is done using value-based checking. This checking evaluates each of the values, and if the value difference is more than a given threshold, then only the values are passed to the network. Due to this, the delay is reduced by more than 40% when compared to IoT-Data oriented map, D-Fog and fuzzy C-means methods, while the failure probability is reduced by 60% over the course of 1000s of requests. This framework has optimum quality of service (QoS) performance but has limited privacy. The work in [4] can be used in order to improve on this. It proposes a distributed access control system using blockchain. It uses mixed linear and nonlinear spatiotemporal chaotic systems and least significant bit (LSB) based system for data encryption. While to control access, the attribute-based access control mechanism is used. This mechanism can be observed from figure 3, wherein the resource being accessed and the data being communicated can be seen to be passed through different control blocks. The AAR block or Attribute-based Access Request block, originates the request for data access.

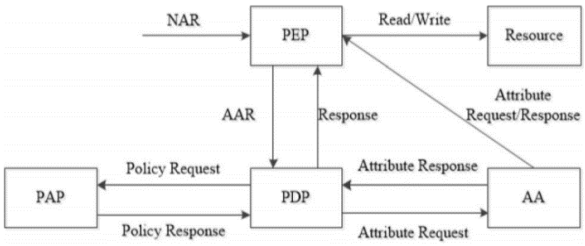

Figure 3. Attribute based access control

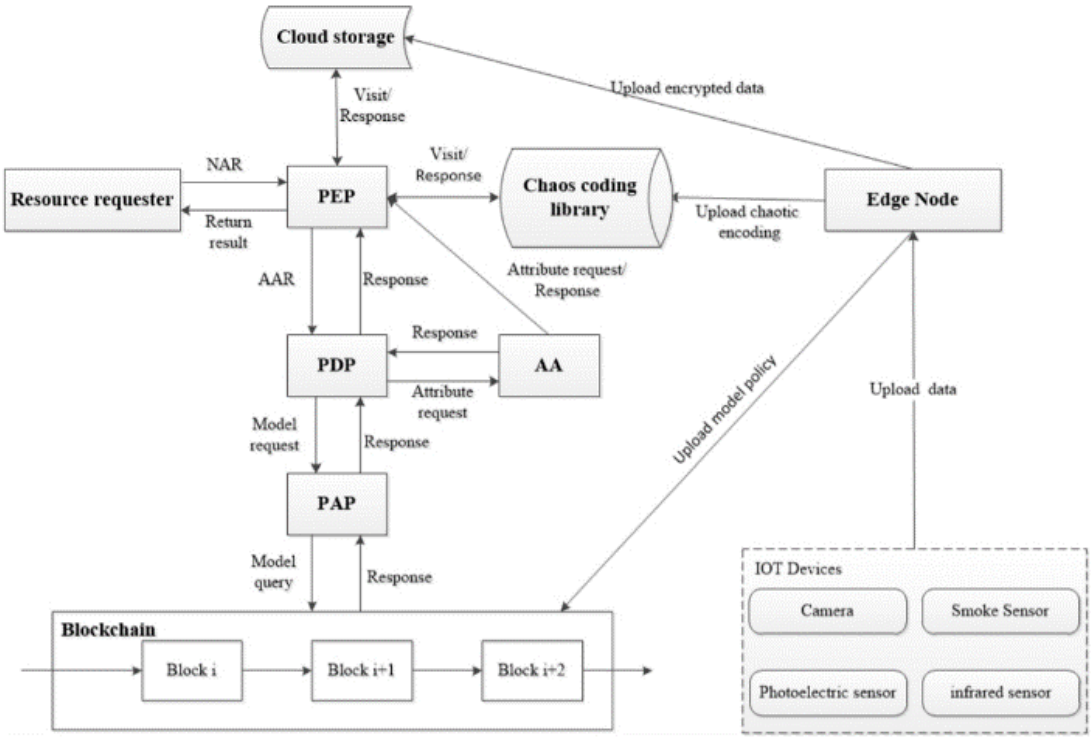

Figure 4. Blockchain data storage framework

The PEP or policy enforcement point enforces policies setup by the policy decision point (PDP), whose main function is to generate rules in the network. Policy management point manages these policies, and the attribute authority is responsible to manage attribute-based access in the system. This model is incorporated using a blockchain-powered system using the flow observed in figure 4, wherein data from the chaotic encoding library is given to the edge node for storage on the blockchain network.

This system has high security, and is double tamper proof, due to blockchain and chaos coding respectively. Another zoning-based blockchain powered secure IoT network can be observed from [5], wherein Ethereum blockchain is used for block storage and retrieval. The overall flow of data storage and retrieval can be observed from figure 5, wherein data manufacturers generate the data, which is consumed by the users using a smart-contract architecture with decentralized cloud.

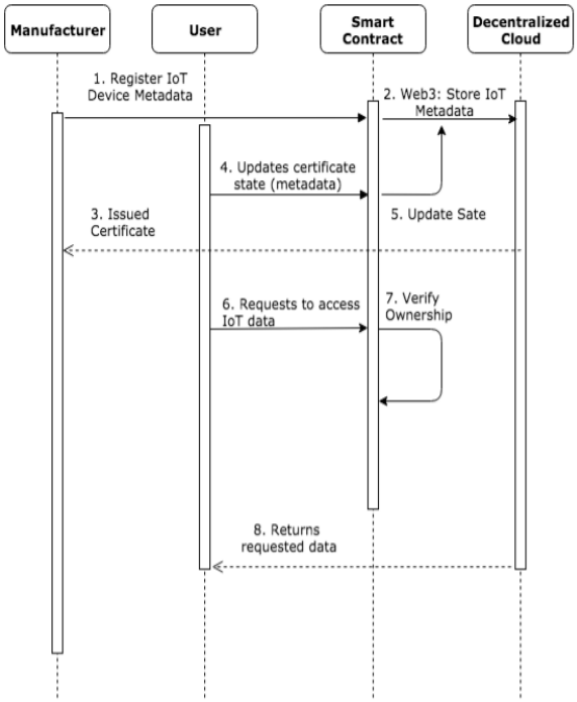

Figure 5. Ethereum-based IoT data storage

The smart contract based Ethereum blockchain increases the delay of block storage and retrieval, while comparative analysis about this delay is not provided, but a value of 16 seconds for 500 kB of blockchain data writing is very high for real-time purposes. In order to improve the performance of this blockchain, the work in [6] must be considered. It uses a mining framework for managing the data storage using a reward mechanism. Due to this mechanism the delay of operation is reduced, and the overall service quality is improved.

IoT applications have vastly entered into the Industry 4.0 era. These applications require high security and full proof checking of the system before actual deployment. The work in [7] introduces Compressed and Private Data Sharing (CPDS) in order to effectively manage industrial data. The overall working of CPDS can be observed from figure 6, wherein specific blockchain access control tokens are given to industrial participants and third-party users. The access control manager defines roles for the users and provides access keys for the requesting parties. It uses the Ciphertext-Policy Attribute-Based Encryption (CP ABE) algorithm for securing data communication between each of the users of the network.

The data from each of the users is aggregated and finally compressed using a Tree-based data compression mechanism as observed from figure 7. This mechanism divides the data into different trees and compresses redundant or non-useful information as per the given application. Each of the point transactions are stored in the blockchain directly, while the data transactions are compressed and then stored into the chain.

ISSN 2319–7757 EISSN 2319–7765 I OPEN ACCESS

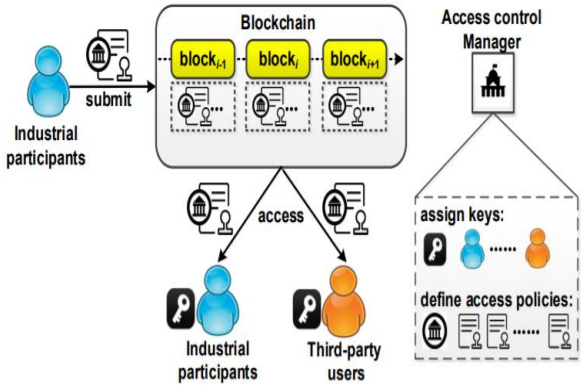

Figure 6. Overview of CPDS

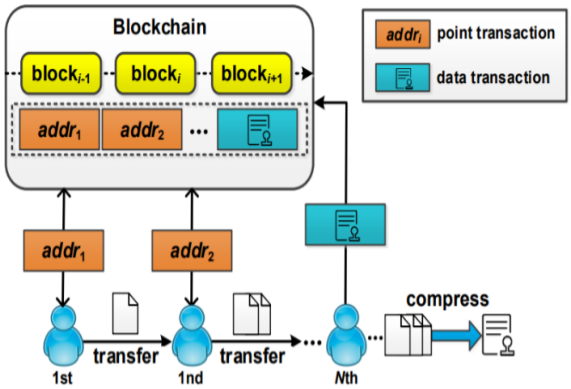

Figure 7. Tree-based compression

Due to this, the delay of storage and retrieval is reduced by almost 80% when compared to a non-blockchain and non-compression system architecture. Moreover, this technique can be further enhanced with the help of data analytics embedded into the blockchain as suggested in [8]. The work in [8] uses deep learning to reduce data storage either via location-based reduction or similarity-based reduction. The process of this reduction can be observed from figure 8 (a) and 8 (b), wherein data reduction is performed on the edge nodes, and the aggregated data is pushed onto the cloud.

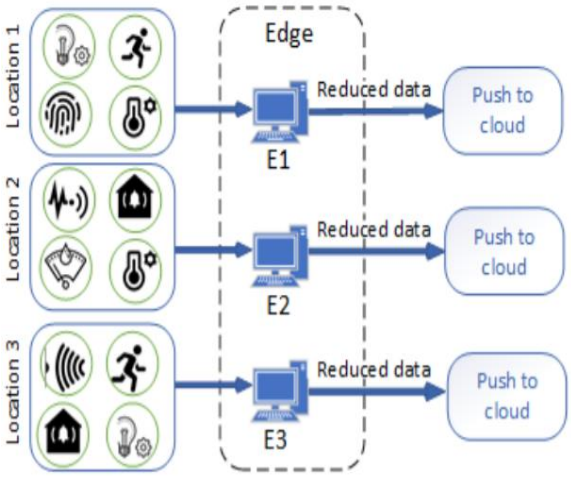

Figure 8 (a) Location based reduction

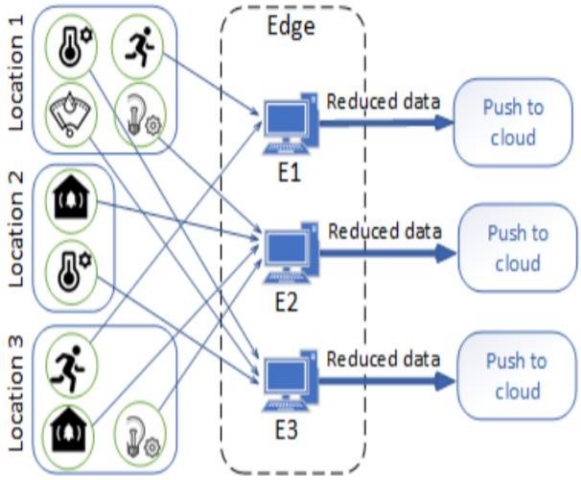

Figure 8 (b) Value based reduction

Due to multiple-kinds of data reduction techniques there is a performance improvement of 70% when compared to non-reduction counterpart systems. Due to data reduction usually, there are chances of data loss, but this technique is able to reproduce the data with almost 100% accuracy. These claims must be verified before actual implementation.

Another blockchain-powered system is described in [9], wherein public auditing is done for large scale IoT applications. This system is shielded against 51% attack and can also remove any kind of malicious entities which might accidently join the system. The proposed auditing scheme can be observed from figure 9, wherein file-splitting and Merkle root calculations are done in order to improve the auditing process. This auditing process makes the system immune to attacks, as there is 100% data transparency along with high energy efficiency. The energy efficiency is achieved due to distributed processing of blocks. But the network faces issues like limited data dissemination capabilities, and reduced speed of operation.

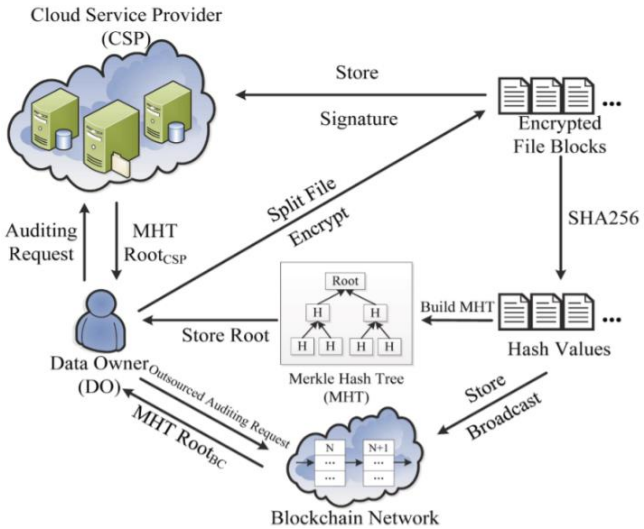

Figure 9. The public auditing process

The data dissemination efficiency can be improved with the help of the work in [10], wherein Polymorphic Erasure Coding with Markov decision Adaptability and Neural networks (PECMAN) is proposed. The PECMAN algorithm reduces the delay, optimizes the deployment cost and reduces the overheads of the IoT system when compared with Polynomial-time Optimal Storage Allocation (OSA), Multi-user Shared Access (EMUSA) and Event-Aware Back pressure Scheduling Scheme (EABS). The work uses an offloaded Adaptive Markov decision process which performs all the transmission and data control processes, which is followed by an offloaded neural network to perform network coding. The encryption and decryption are done using Polymorphic Erasure Coding (PEC), which enhances the network performance via low complexity encoding and decoding processes. Due to a series of such algorithms, the overall IoT device activations improve by 10%, wherein more than 95% of IoT devices can be activated in the system with a collision rate of less than 0.001 (0.1%). This enables the underlying implementation to be deployed for real-time

ISSN 2319–7757 EISSN 2319–7765 I OPEN ACCESS

networks. This system can utilize the study in [11] in order to further improve its data dissemination and control processes. While the system in [10] is very secure due to PEC, its security can be further enhanced with the help of artificial intelligence techniques as mentioned in [12]. Techniques like Additive perturbation, Multiplication perturbation, ObfNet, etc. can be deployed to improve privacy, while HTTPS protocol, Blockchain and HMAC technology can be used for Authentication management. Deffie Hellman (DH) key exchange, with ECC asymmetric encryption must be used for improving Confidentiality and reliability of IoT data, while deep reinforcement learning must be used for collection and share of IIoT (Industrial IoT) data. Structural methods like Blockchain ledger can be deployed for Edge computing offloading, while Game theory can be used to enhance the performance of Multi-hop computing offloading.

Improving data storage security for big-data platforms is of utmost importance when industrial applications are considered. The work in [13] proposes an Ant Colony (ACO) based method that combines Hadoop file system (HDFS) and Google file system (GFS) for storage of IoT data. It is observed that using the ACO algorithm for selection between HDFS and GFS, the task execution delay is reduced by 20% when compared to only HDFS and only GFS storage systems. This concept can be easily extended to other security frameworks, for instance the work in [14] extends the data storage framework to enterprise multimedia data. It also proposes Master Encryption Key (MEK) algorithm combined with Advanced Encryption Standard (AES) for improving the overall security of multi-media data storage. This system can be observed from figure 10, wherein a 2-step authentication framework along with cloud storage are integrated for improved multimedia storage performance. Due to this combination attacks like Collude Attack, Dictionary Attack, Malicious Cloud Service Provider, Data Modification Attack, Identity and Password Theft Attack, Compromised Key Attack, Denial of Service Attack and Ping of Death and ICMP Attack are removed from the system. This improves the system security but makes the system performance moderate in terms of delay needed for data searching when requested by the users. This drawback can be reduced by using aggregation and compression techniques are mentioned previously in [1] and [7].

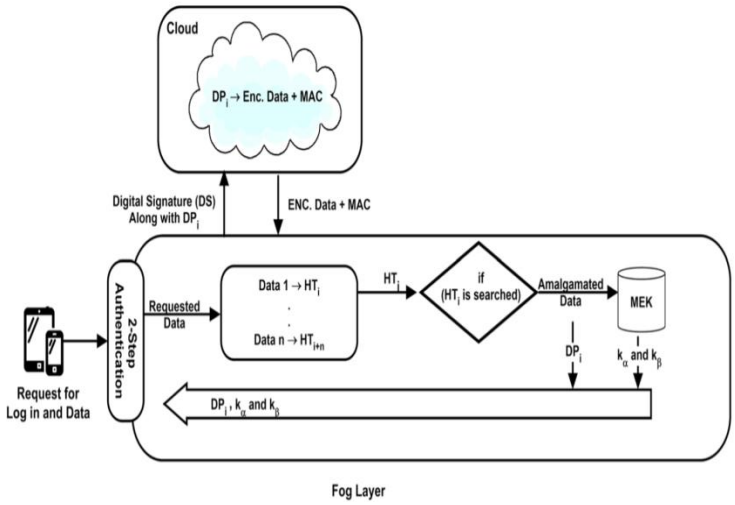

Figure 10. MEK with AES for secure data storage

The work in [15] analyses the effect of using Java Simple Object Notation (JSON) for storing IoT data. It uses the Smart Appliances Reference (SAREF) ontology for evaluating the performance of JSON for IoT semantic interoperability. They conclude that the light weighted JSON-LD (linked data) framework is faster than JSON and must be used for IoT data storage and retrieval applications. An application of such a data representation system can be observed from [16], wherein an Industrial IoT-Based Monitoring System for Power Substations is designed. They suggest that the designed system is able to handle real-time IoT data and improve the delay performance with the help of light-weighted data presentation frameworks. Other light-weighted data storage architectures are presented and compared in [17], wherein the following algorithms are described,

- Handle system that uses 2-step algorithm for information searching via Global and Local handle registries

- A Data-oriented network architecture (DONA) hashing and public key crypto-systems are used for data communication
- Distributed hash table (DHT) uses a decentralized solution for hashing and processing data

These algorithms use Data Record (DR), Routing Record (RR) or Dynamic Routing Record (DRR) packets for searching the stored information. A combination of the searching and data representation protocols is also compared in [17], wherein it is observed that a combination of Chord with DR and DRR improves the performance of IoT data storage in terms of routing delay, routing load and cache hit ratio for the system. This QoS can be further improved with the help of cluster management in fog nodes as described in [18], wherein the utility of fog nodes for data processing is showcased. This utility is improved due to the usage of node clustering, and assigning closest-to-sensor nodes for final job execution. Application of these algorithms for deploying nodes at cultural heritage sites can be observed from [19], wherein IoT sensors are deployed at cultural heritage sites and an image processing application is deployed to test the efficiency of the deployed sensors. Analytics like number of visitors, number of scans, etc. are performed with the help of data mining algorithms. This application can be extended to Cognitive IoT (C-IoT) scenarios as observed from [20], wherein IoT nodes are divided into primary and secondary nodes. Each of these nodes have different data access patterns, and thus enable the network to provide higher QoS when primary sensors are being queried, while a lower QoS is provided when secondary sensors are being queried. This enables the network to have better lifetime and lower delay whenever needed.

Low power data analytics always assist IoT systems by providing high level of abstraction with low energy consumption. For instance, the work in [21] proposes a collective execution engine that allows IoT devices to collectively execute process data in order to save energy. This allows the devices to work in combination for executing a single task, and finally aggregate the data over the cloud. An example of such a system can be observed from figure 11, wherein fitness data and camera data are processed on collective devices. The final results are data is stored on these devices before uploading to the cloud.

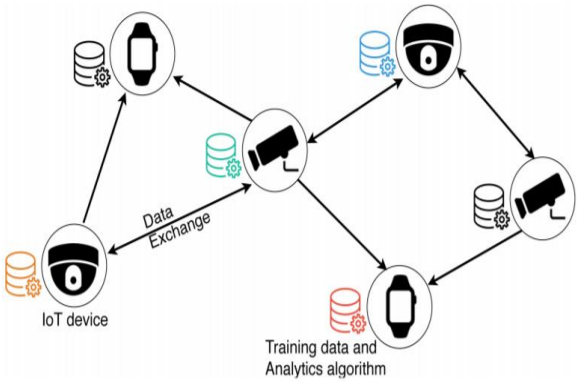

Figure 11. Collective data processing

Due to this, the overall delay is reduced to about 0.41 seconds as compared with 0.76 seconds when processed on single devices, while reducing the power consumption to 0.09 W from 0.12 W. This allows the IoT devices to have predictive analysis capabilities. These capabilities assist the IoT devices to enhance their performance via predicting the behaviour of sensing and access patterns. The work in [22] proposes such an architecture which can be observed from figure 12, wherein IoT gathers data from sensors, which is given to a clustering algorithm for division into different groups. Each of these groups are given to association rule mining block, wherein prediction rules are evaluated. Algorithms like apriori, SPAM, etc. are applied here. Finally, outlier analysis and post-processing is done in order to produce the final predictive rules for the system.

The application of such a system can be observed in [23], wherein a smart metering system is deployed using predictive analysis. Due to which the final energy consumption and delay are reduced by over 10% when compared to their non-predictive layer counterparts. A similar system applied to healthcare is deployed in [24], which also suggests that predictive modelling is very effective when applied to IoT devices. The predictive engine can be offloaded to the cloud for further improvement in the performance. Due to offloading an improvement of more than 20% in terms of computational efficiency can be observed from [25]. Some IoT applications make use of this offloading to improve the delay and energy performance. Such a system is depicted in [26], wherein a smart city design is discussed. Using this design along with named-data-networking and peer-to-peer (P2P) computations the final system is deployed. This system is an upgrade over the existing non-P2P systems.

ISSN 2319–7757 EISSN 2319–7765 I OPEN ACCESS

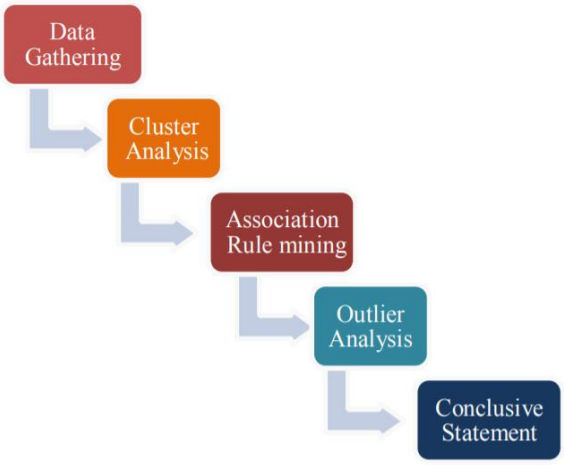

Figure 12. Predictive analysis in IoT

For big data applications, several IoT software modelling tools are also available. A survey of these tools can be found in [27], wherein it can be observed the IoT data management and analysis is a very upcoming field, and standards are yet to be finalized for the same. These standards are in terms of data representation, storage and analysis. Each research article proposes a different system which has some level of efficiency in one or more parameters by compromising other parameters. This efficiency can be optimized without sacrificing other parameters. For instance, the work in [28] uses a scalable and configurable end-to-end data collection and data analysis system. This system utilizes standardized architectures for security, data collection, data analysis and data communication. An example of a standard security module can be observed in figure 13, wherein rule-based cryptography is used for improved security in the IoT system during data capture phase.

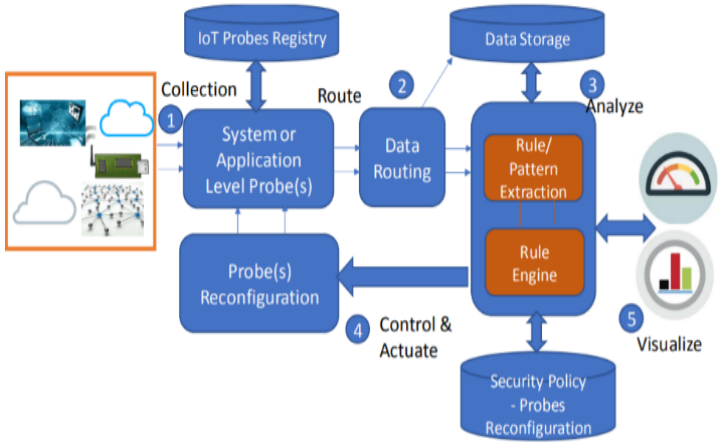

Figure 13. Security during data capture

Due to this standardization the system is highly flexible, and thus can be used for future proof systems. Parametric analysis of such systems is a must, thus the work in [29] proposes a set of parameters which can be evaluated to test the efficiency of any IoT deployment. It proposes a novel system to evaluate IoT networks, which can be observed from figure 14, wherein edge devices generate the data. This data is processed by the core-system, which has data mining, statistical analysis and machine learning modules. Finally, the application module provides access to these systems via an application programming interface (API). Such standardizations in terms of performance evaluation are needed so that the final system can be flexible and can be deployable for any set of given application constraints.

ISSN 2319–7757 EISSN 2319–7765 I OPEN ACCESS

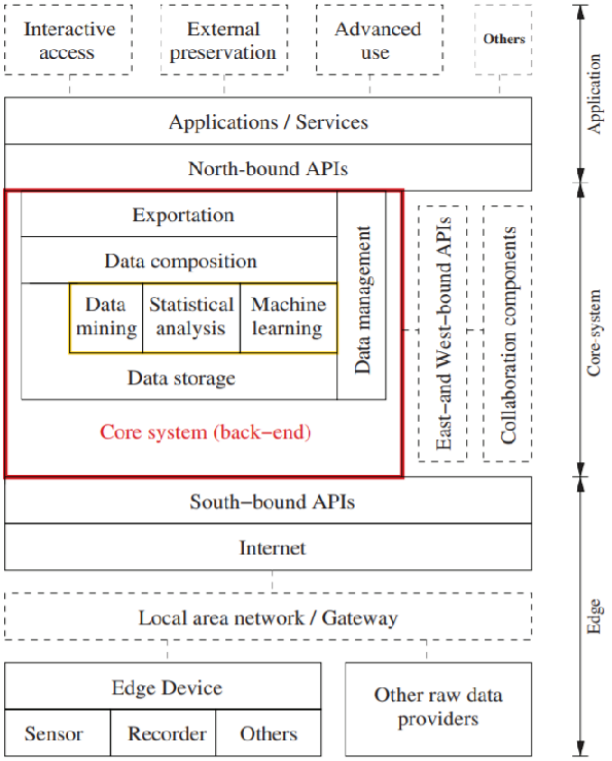

Figure 14. IoT analysis architecture

Such architectures allow for systems to deploy their software processing modules either on the IoT node, the edge node or the cloud itself. The work in [30] indicates a set of architectures which can be used in order to deploy the modules on edge devices and discusses various applications of doing the same. Edge computing can be used for applications like health care, video analysis, vehicle interconnection, Mobile big data analysis, Intelligent building control, Marine monitoring and control, smart home and smart city. Each of these applications must be deployed with edge nodes as offloading nodes for an efficient IoT deployment. A set of privacy policies and their analysis can be observed from [31], these policies must be studied and used whenever large-scale IoT applications are being designed. The work in [32], [33] also analysis the effect of fog and edge devices on data analytics in IoT. These applications suggest that any kind of data processing must be done on the device itself, but if the required application demands higher memory or computational power, then these computations must be offloaded to the edge and fog devices. A statistical analysis of these techniques can be observed from the next section.

3. STATISTICAL ANALYSIS

In order to perform statistical analysis of the reviewed IoT data representation and analysis architectures some common parameters were required. These common parameters include security level (SL), data access delay (DA), data writing delay (DW) and flexibility to interface with other systems (F). A comparative analysis of the systems on these parameters can be observed from table 1, wherein parameter values are converted into fuzzy levels. The nomenclature of these levels is at par with the standard fuzzy nomenclature, wherein Low (L), Medium (M), High (H) and a Very (V) clause is added depending upon the strength of these values observed in the review. This fuzzy level comparison is done because most of these systems are not implemented using standard performance test beds, which is also one of the research gaps in the field of IoT system development.

Table 1. Statistical analysis of different IoT architectures

Work	SL	DA	DW	F
Keccak-Chaotic [1]	H	M	H	H
Fast retrieval [2]	M	L	M	M
Data Agg with off-loading [3]	H	M	M	H
Privacy protect [4]	VH	H	H	L

ISSN 2319–7757 EISSN 2319–7765 I OPEN ACCESS

Block-chain [5]	H	M	H	M
Block-chain for large scale IoT [6]	H	M	H	L
CPDS [7]	H	L	M	H
Edge process with deep learning [8]	M	L	M	H
Public auditing [9]	VH	L	L	H
Data dissem-ination [10]	M	L	M	H
Hadoop IoT [13]	M	L	L	M
Mobile fog [14]	H	L	M	M
Semantic JSON [15]	M	L	L	H
Efficient storage [17]	M	L	L	M
Fog compute [18]	M	L	L	H
C-IoT [20]	M	L	M	M
Co-operative edge [21]	M	L	M	VH
Predictive analysis [22]	M	L	H	H
Mobile cloud big data [25]	M	L	M	H
Smart city [26]	H	L	M	H
E2E collection and analysis [27]	M	L	M	H
Fog data analytics [32]	M	L	M	M
Fog for health care [33]	M	L	M	M

From the analysis it can be observed that all of the blockchain powered IoT data representation standards have high security. But due to block writing delays the data writing capabilities are limited, which increases the communication delay of the network. Techniques that use peer to peer communication models are found to be very scalable in terms of interoperability with other entities. A combination of these models must be done in order to develop a highly efficient, low delay and high throughput system.

4. CONCLUSION AND FUTURE WORK

Considering the different parameters analyzed for various IoT systems, it can be observed that CPDS and public auditing methods offer highly scalable architectures. The scalability is further enhanced using co-operative edge computing devices. Thus, for an IoT system to be most effective in terms of inter-operability and flexibility, they must represent their data using either the CPDS or the co-operative architectures presented in the research. Moreover, data analysis must be done using fog or edge computing devices for highest efficiency. Data dissemination is one of the most effective approaches for transferring data in order to perform data analysis, and thus must be used for IoT powered systems. For data representation and storage in IoT, blockchain-based systems are most useful. They provide high security, low reading delays and maintain high privacy between networks of different genre. Moreover, blockchain networks can be further divided into sidechain-based networks for improved performance. This technology can be explored in future for design of high security IoT systems.

Funding:
This study has not received any external funding.

Conflict of Interest:
The authors declare that there are no conflicts of interests.

Data and materials availability
All data associated with this study are present in the paper.

REFERENCES AND NOTES

1. Ravikumar, S., Kavitha, D. (2020). IoT based home monitoring system with secure data storage by Keccak–Chaotic sequence in cloud server. Journal of Ambient Intelligence and Humanized Computing. https://doi.org/10.1007/s12652-020-02424-x.

2. Chen. J., Yin. L., Zhang. T., Liu. Y., Deng. Z. Data Storage Method for Fast Retrieval in IoT.
3. Alfarraj O. (2020): A machine learning-assisted data aggregation and offloading system for cloud–IoT communication. Peer-to-Peer Networking and Applications, Springer, https://doi.org/10.1007/s12083-020-01014-0.
4. Liu, Y., Zhang, J., & Zhan, J. (2020). Privacy protection for fog computing and the internet of things data based on blockchain. Cluster Computing. https://doi.org/10.1007/s10586-020-03190-3.
5. Thakker, J., Chang, I., & Park, Y. (2020). Secure Data Management in Internet-of-Things Based on Blockchain. 2020 IEEE International Conference on Consumer Electronics (ICCE). Retrieved 21 December 2020, from.
6. Li, R., Song, T., Mei, B., Li, H., Cheng, X., & Sun, L. (2019). Blockchain for Large-Scale Internet of Things Data Storage and Protection. IEEE Transactions on Services Computing, 12(5), 762-771. https://doi.org/10.1109/tsc.2018.2853167.
7. Qi, S., Lu, Y., Zheng, Y., Li, Y., & Chen, X. (2020). Cpds: Enabling Compressed and Private Data Sharing for Industrial IoT over Blockchain. IEEE Transactions on Industrial Informatics, 1-1. https://doi.org/10.1109/tii.2020.2998166.
8. Ghosh, A., & Grolinger, K. (2020). Edge-Cloud Computing for IoT Data Analytics: Embedding Intelligence in the Edge with Deep Learning. IEEE Transactions on Industrial Informatics, 1-1. https://doi.org/10.1109/tii.2020.3008711
9. Li, J., Wu, J., Jiang, G., & Srikanthan, T. (2020). Blockchain-based public auditing for big data in cloud storage. Information Processing & Management, 57(6), 102382. https://doi.org/10.1016/j.ipm.2020.102382
10. Rathanasalam, R., & Kanagasabai, K. (2020). Data dissemination with interoperability in IoT network. International Journal of Communication Systems, e4513. https://doi.org/10.1002/dac.4513
11. Krishna, P., Yenduri, S., & Ariwa, E. (2020). Data analytics in wireless systems and IoT issues and challenges. International Journal of Communication Systems, 33(13), e4522. https://doi.org/10.1002/dac.4522
12. Xu, Z., Liu, W., Huang, J., Yang, C., Lu, J., & Tan, H. (2020). Artificial Intelligence for Securing IoT Services in Edge Computing: A Survey. Security and Communication Networks, 2020, 1-13. https://doi.org/10.1155/2020/8872586.
13. Mo, Y. (2019). A Data Security Storage Method for IoT under Hadoop Cloud Computing Platform. International Journal Of Wireless Information Networks, 26(3), 152-157. https://doi.org/10.1007/s10776-019-00434-x
14. Sood, S. (2019). Mobile fog based secure cloud-IoT framework for enterprise multimedia security. Multimedia Tools And Applications, 79(15-16), 10717-10732. https://doi.org/10.1007/s11042-019-08573-2
15. MOREIRA, J., PIRES, L., & SINDEREN, M. (2020). Semantic Interoperability for the IoT: Analysis of JSON for Linked Data. In Semantic Interoperability for the IoT: Analysis of JSON for Linked Data (pp. 163 - 169). ISTE Ltd and John Wiley & Sons, Inc. Retrieved 21 December 2020, from.
16. Zhao, L., Brandao Machado Matsuo, I., Zhou, Y., & Lee, W. (2019). Design of an Industrial IoT-Based Monitoring System for Power Substations. IEEE Transactions on Industry Applications, 55(6), 5666-5674. https://doi.org/10.1109/tia.2019.2940668
17. Karolewicz. K., Beben A., Mongay Batalla M., Mastorakis G., X. Mavromoustakis C. (2016). INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT. Published online in Wiley Online Library (wileyonlinelibrary.com) DOI: 10.1002/nem.1932.
18. Akhare, R., Mangla, M., Deokar, S., Wadhwa, V. (2020). Springer Nature Singapore Pte Ltd. 2020. S. Tanwar (ed.), Fog Data Analytics for IoT Applications, Studies in Big Data 76, https://doi.org/10.1007/978-981-15-6044-6_7.
19. Piccialli, F., Benedusi, P., Carratore L., Colecchia, L. (2020). An IoT data analytics approach for cultural heritage. Personal and Ubiquitous Computing https://doi.org/10.1007/s00779-019-01323-z
20. SASSI, H., GHOZZI JEDIDI F., CHAARI FOURATI, L. (2019). A New Architecture for Cognitive Internet of Things and Big Data, International Conference on Knowledge-Based and Intelligent Information & Engineering Systems. Peer-review under responsibility of KES International. 10.1016/j.procs.2019.09.208.
21. Galanopoulos, A., Salonidisy,T., Losifidis, G.(2020). Cooperative Edge Computing of Data Analytics for the Internet of Things. IEEE Transactions on Cognitive Communications and Networking. DOI 10.1109/TCCN.2020.3019610.
22. Taneja, T., Jatin, A., Dr. Bajaj, S., Predictive Analytics on IOT. International Conference on Computing, Communication and Automation (ICCCA2017). ISBN:978-1-5090-6471-7/17/$31.00 ©2017 IEEE.
23. Hu, H., Tang, L. (2020). Edge Intelligence for Real-Time Data Analytics in an IoT-Based Smart Metering System. Emerging intelligent systems and smart computational technologies for future IOT. Digital Object Identifier: 10.1109/MNET.011.2000039.
24. S. Arulananda Jothi, S., Abdul Samath, J., Anandharaj, K. (2019). A Study On Iot And Data Analytics In Healthcare Systems. International Journal of Scientific & Technology Research Volume 8, Issue 10, October 2019.
25. Kchaou, H., Kechaou, Z., M. Alimi, A. (2015). Towards an offloading framework based on Big Data analytics in Mobile

ISSN 2319–7757 EISSN 2319–7765 | OPEN ACCESS

Cloud Computing Environments. Procedia Computer Science Volume 53, 2015, Pages 292–297. 2015 INNS Conference on Big Data. doi: 10.1016/j.procs.2015.07.306.

26. Shih,C. S., Lee,K. H., Chou, J.J., Lin, K. J. (2017). Data-driven IoT applications design for smart city and smart buildings, *IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (Smart World/SCALCOM/UIC/ATC/CBD Com/IOP/SCI)*, San Francisco, CA, 2017, pp. 1-8, doi: 10.1109/UIC-ATC.2017.8397394.
27. Wang, Y. Nazir Jan, M., Chu, S., Zhu, Y. (2020). Use of Big Data Tools and Industrial Internet of Things: An Overview. Hindawi Scientific Programming, Volume 2020, Article ID 8810634, 10 pages https://doi.org/10.1155/2020/8810634.
28. Roukounaki, A., Efremidis, S., John, S, Neises, J., Walloschke, T., Kefalakis, N.(2019). Scalable and Configurable End-to-End Collection and Analysis of IoT Security Data: Towards End-to-End Security in IoT Systems," *2019 Global IoT Summit (GIoTS)*, Aarhus, Denmark, pp. 1-6, DOI: 10.1109/GIOTS.2019.8766407.
29. Tsai, C. W., Tsai P. W., Chiang, M. C., Yang C. S., (2018) Data analytics for internet of things: A review, WIRES Data Mining & Knowledge Discovery. DOI: 10.1002/widm.1261.
30. Wang, S. (2019). Edge Computing: Applications, State-of-the-Art and Challenges Advances in Networks 2019; 7(1): 8-15 http://www.sciencepublishinggroup.com/j/net; doi: 10.11648/j.net.20190701.12 ISSN: 2326-9766 (Print); ISSN: 2326-9782 (Online).
31. Perez, A. J., Zeadally, S., Cochran, J., (2018). A review and an empirical analysis of privacy policy and notices for consumer Internet of things, Wiley, DOI: 10.1002/spy2.15.
32. Modi, A., Jani, S., Chauhan, K., Bhatia, K. (2020). Process Model for Fog Data Analytics for IoT Applications, Springer Nature Singapore Pte Ltd. 2020. S. Tanwar (ed.), Fog Data Analytics for IoT Applications, Studies in Big Data 76, https://doi.org/10.1007/978-981-15-6044-6_9.
33. Vyas, T., Desai, S. Ruparelia, A. (2020). Fog Data Processing and Analytics for Health Care-Based IoT Applications Springer Nature Singapore Pte Ltd. 2020. S. Tanwar (ed.), Fog Data Analytics for IoT Applications, Studies in Big Data 76, https://doi.org/10.1007/978-981-15-6044-6_18.

ISSN 2319–7757 EISSN 2319–7765 | OPEN ACCESS