ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8

International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies

http://TuEngr.com

Using Blockchain Technology to Secure Data of IoT

Khaled Mofawiz Alfawaz[1*]

[1] *Management Information System Department, Faculty of Economics and Administration, King Abdulaziz University, Jeddah, SAUDI ARABIA.*

**Corresponding Author (Email: kalfawaz@kau.edu.sa).*

Paper ID: 12A13B

Volume 12 Issue 13

Received 29 June 2021
Received in revised form 14 September 2021
Accepted 22 September 2021
Available online 09 October 2021

Keywords:
Louvain clustering; Louvain algorithm; k-means; IoT blockchain; Security network.

Abstract

In the coming era blockchain and the IoT are going to become the two essential technologies that might have a great role in the organizations and industries such as education, healthcare, governance, commerce, agriculture, and more. IoT has the capability to handle the physical object networks which consist of different enclosed technologies that support communication and interaction or sensors between the internal and external environment. With the changing time, the cost of actuators and sensors are reducing, which intends easy to implement IoT platforms for lots of organizations. A number of healthcare systems are already available with IoT technologies but there a problem arises due to centralized databases. Thus, the data might be vulnerable, also it's difficult for the organizations to store this huge amount of data securely. This study explains the necessity of blockchain technology, blockchain the only the user has complete control over his data. His data cannot be shared without this owner's approval, which is the best part of blockchain technology. Louvain clustering algorithm is introduced.

Disciplinary: Information System, Technology, and Application.

Cite This Article:

Alfawaz, K. M. (2021). Using Blockchain Technology to Secure Data of IoT. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, 12*(13), 12A13B, 1-10. http://TUENGR.COM/V12/12A13B.pdf DOI: 10.14456/ITJEMAST.2021.254

1 Introduction

Internet of Things (IoT) refers to a device of interconnection, internet-related items which have the capability to acquire and switch information over a wireless community or network without human interference. As IoT needs a secure platform for storing data, blockchain is introduced within the IoT. The blockchain is defined as an apparatus of tapping information in a manner that makes it tough or not possible to cheat, commute, or attack the system. Basically, a blockchain is a virtual ledger of transactions this is copied and distributed throughout the whole network of the systems at the blockchain. In the present scenario, blockchain and IoT play a vital role in daily life. As now people are becoming familiar with the concept called IoT, the future will be driven by the IoT. While utilizing IoT, it craves the terms named huge storage and security.

Everything is IoT now, all objects are connected to a network, and the data transmission occurs widely irrespective of time which needs to be stored securely. Imagine if someone ventures into the network and captures every single piece of data, for sure it will create a huge problem. To prevent such a situation, the blockchain is implemented in the IoT concept [1]. There exists a chance of false authentication, device spoofing, less reliability while sharing data. To avoid these privacy concerns and security issues, the centralized server concept is changed and the blockchain technology is included as a section in IoT.

2 BLOCKCHAIN IN IoT

In a heterogeneous network, there is a connection between physical things to communicate which is enabled by IoT. And the information is taken care of by blockchain. The following terms describe how blockchain is used in IoT:

Physical things: In the network, IoT provides a unique id for every distinct thing which is connected to the network which enables the physical things to communicate with the other nodes in the IoT network.

Gateways: gateways are defined as the devices which operate within the cloud and physical things to confirm that the network is established or not and whether security is ensured to the connection.

Networking: This concept is utilized to discover the shortest route within the IoT node and also to have control over the flow of data.

Cloud: Cloud is where the data is computed and stored. The IoT cloud helps IoT devices and applications to have a massive network.

The blockchain is a sequence of cryptographic and accepted blocks of transactions held with the aid of using the node linked in a network. The data of the blocks are saved within the digital ledger which is shared publicly and are distributed. The blockchain offers secure and safe connectivity in IoT networks [1]. With distinctive properties, the blockchain may be a public, consortium, or private.

3 Challenges of Blockchain and IoT

The blockchain and IoT might face some limitations in different categories like storage, privacy, skills, etc. Figure 1 illustrates the challenges of IoT and blockchain [2].

Lack of skills: Since the blockchain is a fresh concept, it is studied by the least number of persons around the globe which is one of the challenges to equip the persons on the blockchain concepts.

Rules and regulations: The IoT and blockchain technologies will be utilized widely in the world thus, it might come across many rules and regulations for performing this concept.

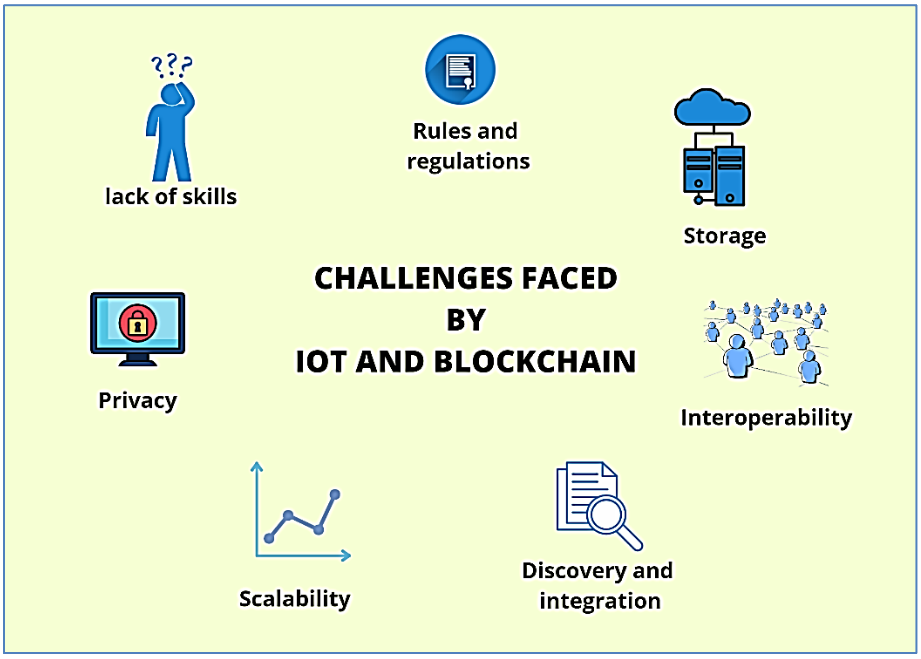

Figure 1: Challenges of IoT and Blockchain.

Storage: Every IoT node stores the digital ledger. Simultaneously, it would improve the storage capacity which will be a challenging situation and might become a huge problem in every connected node.

Interoperability: The term blockchain can be either public or private which leads to another problem called interoperability. So blockchain in IoT has interoperability between private blockchains and public blockchains.

Discovery and integration: Generally, blockchain is never developed for IoT. Which is really an extremely hard operation for the network-connected nodes to find out different nodes in blockchain and IoT. Therefore, IoT-connected nodes can develop each other but then they are not able to integrate and develop the blockchain with another node.

Scalability: Blockchain has a possibility to hang since it is having a very heavy load of transactions. For example, In the year 2019, the bitcoin storage was growing more than 197 GB storage. What if IoT integrates to blockchain? It will again lead to a worse situation.

Privacy: Publicly the ledger is issued to every node connected to the network. While they can access and watch the ledger transactions thus privacy is another challenge in this scenario.

3.1 Problem Analysis from a Dataset

Table 1 contains data about the attacks that occurred in different protocols in the IoT devices. The dataset was named and the files were distinguished to arrange the different cases that occurred during the task [3]. This dataset conveys that the attacks can be performed in various destinations in different time durations. The collected dataset contains many rows, for the approximate analysis, five random rows are chosen and illustrated in a graph (Figure 2).

Table 1: Attacks dataset in different IoT protocols.

UDP	TCP	ICMP
3.244 minutes	4.719 minutes	3.004 minutes
1 minute	5.92 minutes	0.339 seconds
2.798 minutes	3.232 minutes	0.814 seconds
0.343 seconds	5.781 minutes	1.03 minute
5.027 minutes	1.007 minute	4.883 minutes

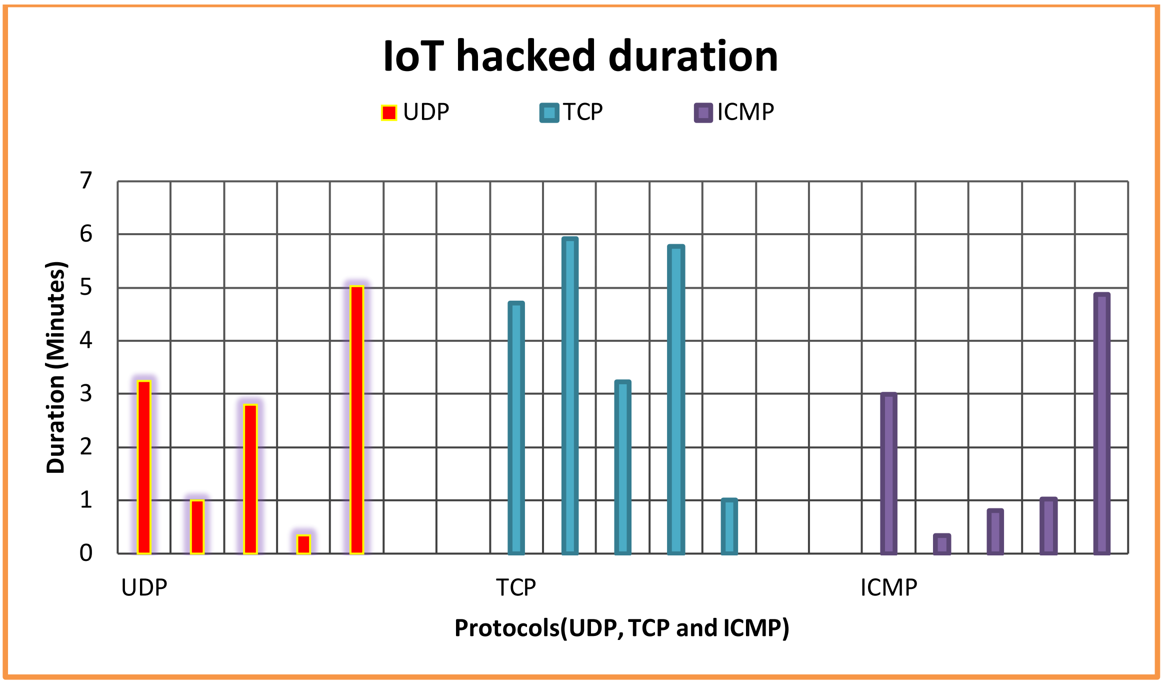

Figure 2: Attack durations in IoT devices

By taking five values from the dataset, figure - 2 is illustrated, where the first five bar shows the attacks occurred in the UDP, second five bars denote attacks on TCP and finally the last five represents attacks in ICMP. As a result, the maximum duration of attacks is experienced in the TCP.

4 Research Methodology

The tool used for data analysis is the orange 3.30.1 version. Orange is a data visualization toolkit and used for interactive data visualization and explorative data analysis. A sample screenshot is given below as Figure 3, which illustrates the workflow of an analysis.

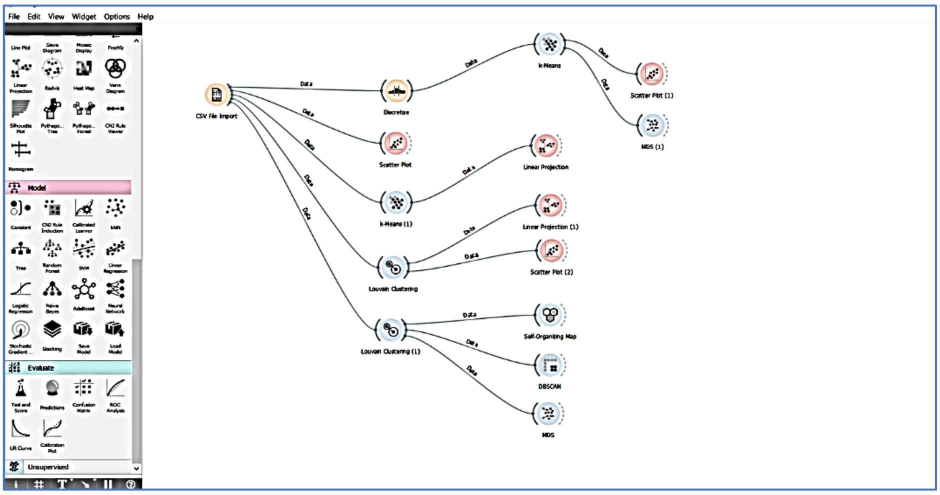

Figure 3: Workflow in orange toolkit.

There are lots of methods and algorithms available in orange such as SVM, Ada booster, Linear regression, PCA, Louvain algorithm, etc.

4.1 Conventional Data Analysis

- K-means is the most common data analysis technique but k-means needs the specified count of clusters i.e., k in advance. It cannot operate with outliers and noisy data.

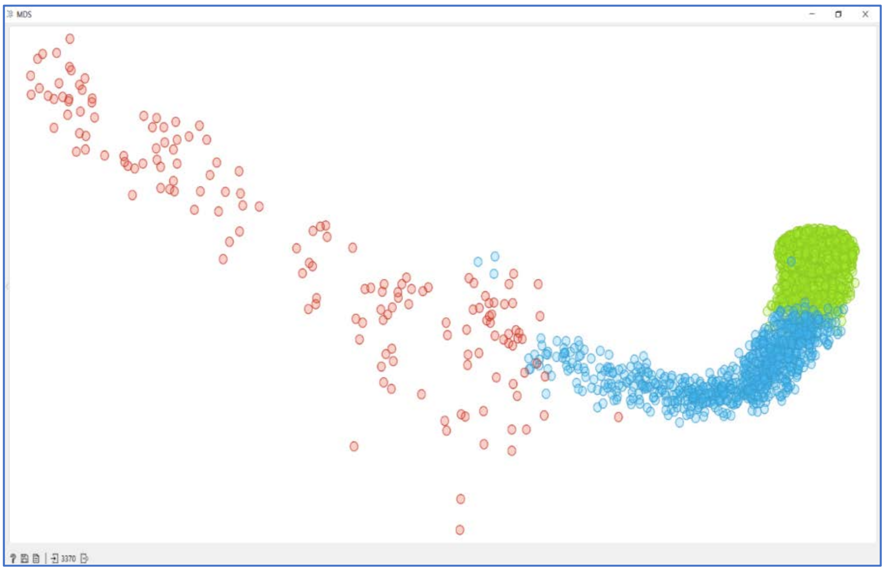

Figure 4: MDS plot

- MDS stands for multidimensional scaling, it is illustrated above in figure – 4, as it is a very basic representation with no specified axis and other information. Thus MDS is one of the least preferred techniques.

5 Data Analysis Using Louvain Clustering Algorithm

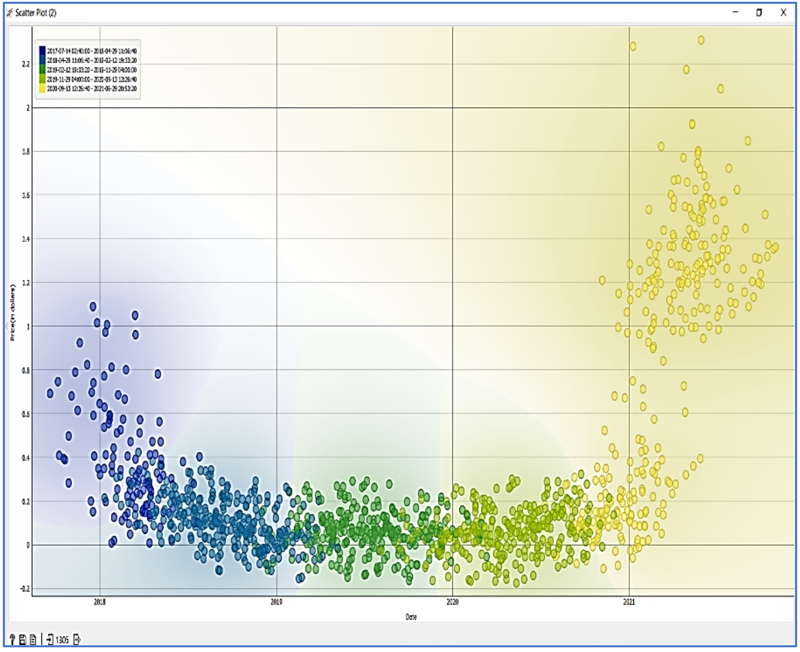

Figure 5: Sample Louvain clustering.

- Figure 5 is a sample screenshot of the Louvain clustering algorithm.
- In a glance, it provides a perfect analysis of unsupervised learning, it has a labelled x and y-axis, colored region, specified range, and values.

5.1 Comparison

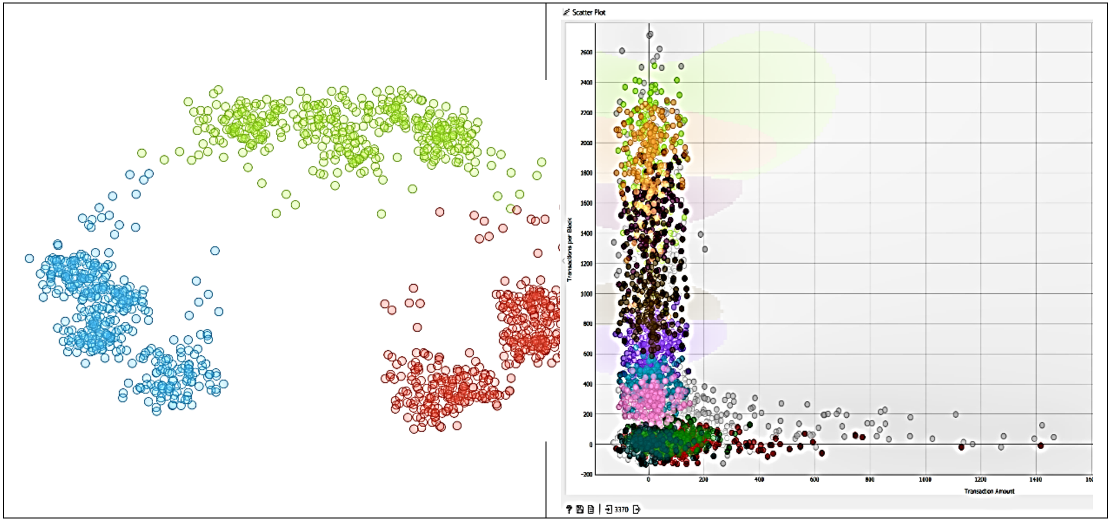

Table 2: Comparison between k-means method and Louvain clustering

- ➢ In general from Table -2, with a comparison to k-means, the Louvain clustering algorithm has the capability to create a more evenly structured cluster.
- ➢ As an inference from a group of Louvain algorithms can develop new clusters whereas k-means algorithm cannot detect it.

6 Experimental Results

This section confirms that the Louvain clustering algorithm operates far better than K-means clustering algorithm. And the Louvain clustering has a definiteness to predict the collection of data, which is not done through K-means clustering.

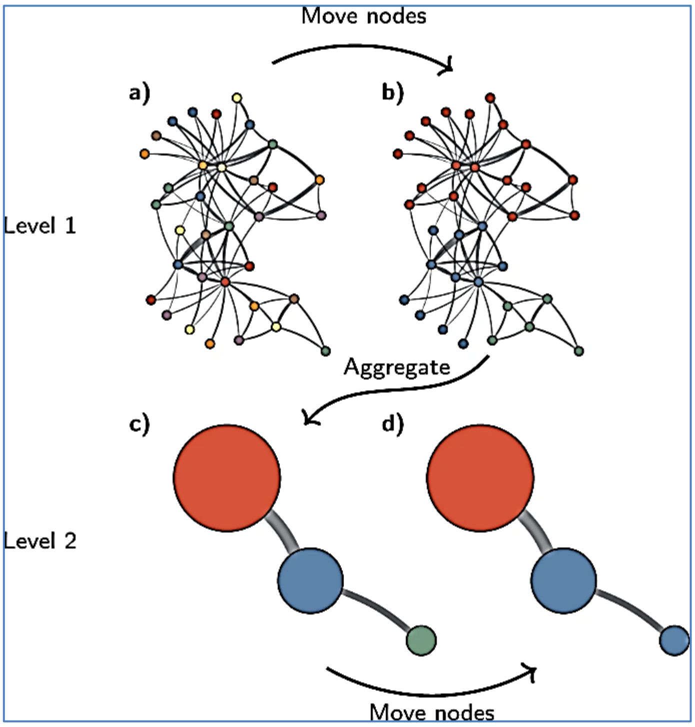

Figure 6: Louvain algorithm.

The Louvain algorithm Figure 6 begins from a singleton partition wherein every node is in its very own network.

a) The algorithm displaces person nodes from one network to another to discover a partition
b) Regarding this partition, an aggregate network is developed
c) The algorithm then displaces person nodes within the aggregate network
d) These steps are repeated till the excellence can't be improved further.

6.1 ALGORITHM

Louvain clustering algorithm is based on resulting the Modularity very efficiently. Modularity Q is calculated as

$$Q = \frac{1}{2m}\sum_{i,j}\left[Aij - \frac{KiKj}{2m}\right]\delta(ci,cj) \quad (1),$$

Where m is the number of links
Aij is the weight of the edge between i and j.
Ki and Kj are degrees of nodes
$\delta(ci,cj)$ implies 1 if $ci = cj$, else it is 0.

STEP 1. To begin, assign every node to a distinct partition or group. The count of partitions is equal to the count of nodes N.

STEP 2. For every consecutive node j, it ensures whether the total value of Q is improving by displacing i from its partition-to-partition.

STEP 3. The node i is then displaced to partition j where the gain of Q is high (positive value). If it's found negative, the original partition label is kept in i.

STEP 4. Now steps 2 and 3 are repeated for every node in sequence(iteration).

STEP 5. The iteration is performed till the value of Q makes any improvement and the main intention is to reach out to a local maximum of Q.

7 Implementation

The above algorithm is implemented for the analysis. Table 3 is a small part of the utilized dataset which is taken from Kaggle.com.

Table 3: BTC Dataset for Py2

Annual Hash Growth	Blockchain Size	Chain Value Density	Daily Transactions	Transaction per block	Transaction Amount
0	4085	0	19	1	0
-84.7634	17214	0	61	1	0
-78.0339	37522	0	94	1	0.537634
-74.5739	59280	0	100	1	1.37234
-70.2886	85810	0	123	1	0
-67.0508	114086	0	130	1	0.472868
-64.9013	144146	0	134	1	2.380952
-60.0583	168000	0	110	1	1.851852
-57.4463	191529	0	109	1	0
-56.6845	215063	0	108	1	1.401869

The column names are as follows:

- Annual hash growth(usage of hashing)
- Blockchain size
- Chain value density
- Daily transactions
- Transaction per block(how much is transferred in one block)
- Transaction amount(count)

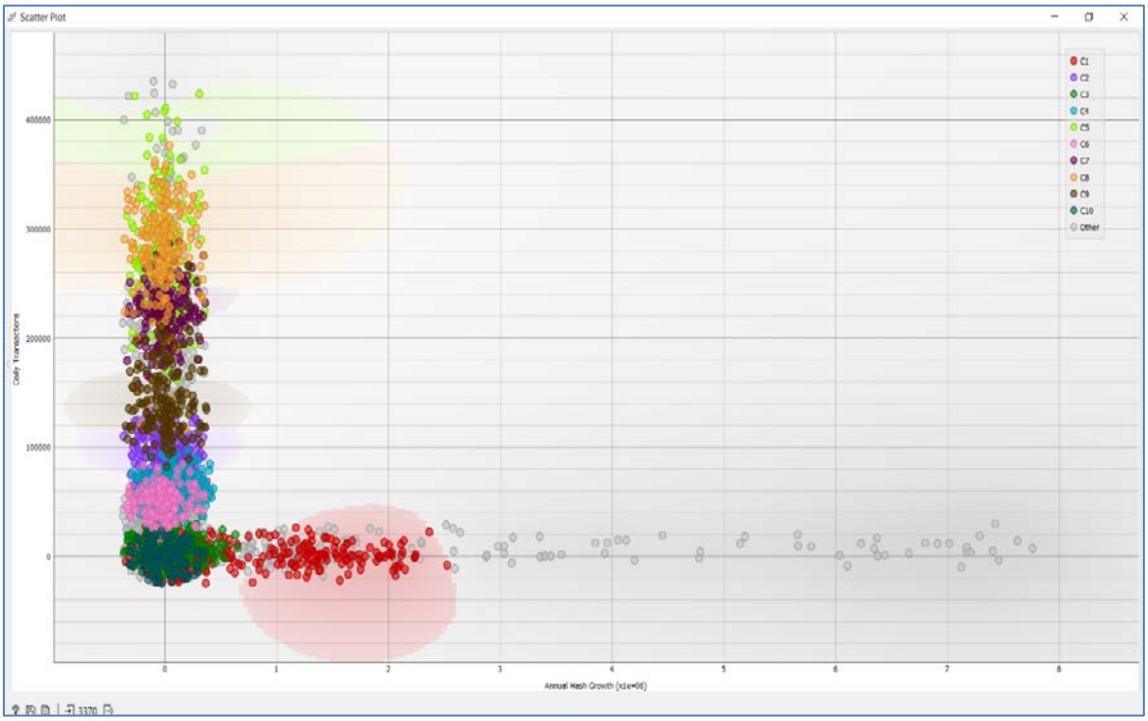

Figure 8: Louvain clustering algorithm(Daily transaction vs Annual hash growth).

Figure 8 displays the importance of hashing since the daily transaction increases with time it is very essential to have a proper hash growth.

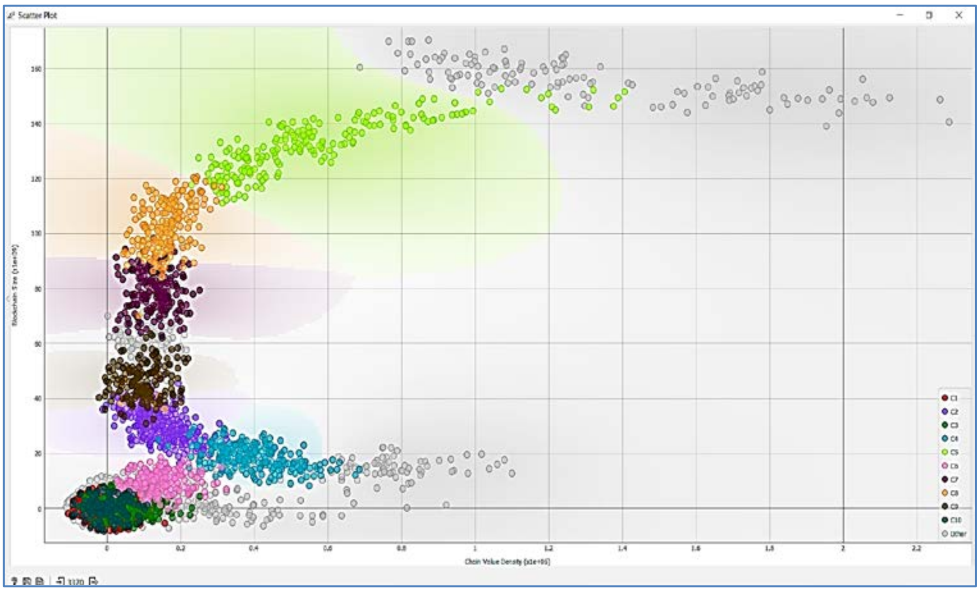

Figure 9: Louvain clustering algorithm(Blockchain size vs Chain value density)

Blockchain size and Chain value density is an important section of blockchain technology. In Figure 9 it is plotted using x and y axis with eleven different colors for each distinct value.

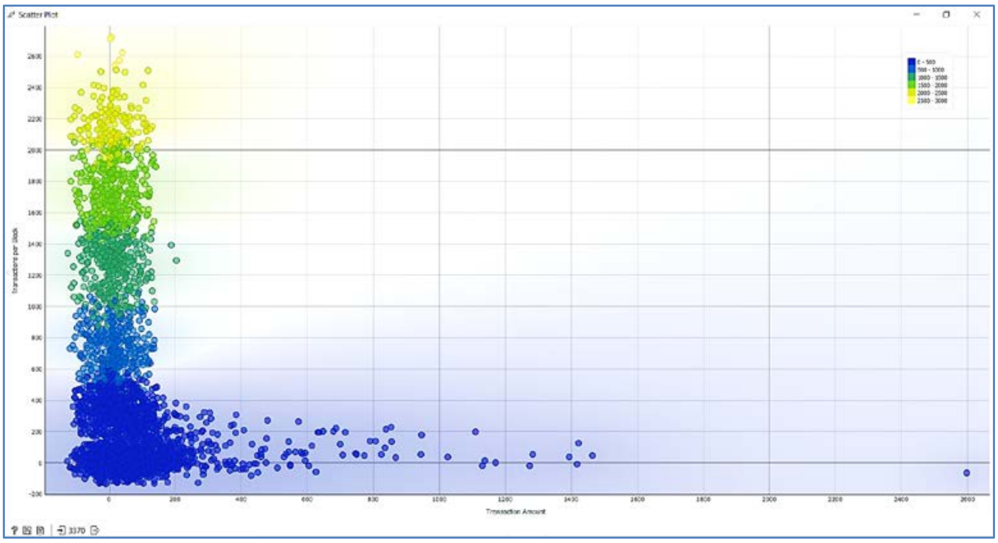

Figure10: Louvain clustering algorithm (Transaction per block vs Transaction amount)

This scatter plot conveys how much is transferred in a block, it also has the x axis and y axis with a small range within a legend. The colored region is also shaded on the grid view. With analysis, the transaction amount is almost a fixed value as compared to the transaction per block.

8 Limitations and Remedies

Companies adopting IoT concepts will continue to face limitations, with a contradiction implementing security technologies and various approaches are enough to find distinct vulnerabilities to IoT.

Blockchain arises with a vital role to prevent those limitations. In an addition, Niche security vendors will be starting to provide those security services, but it still remains a chance of taking a grant of integrity and authenticity services which is supported by the blockchain concepts.

9 Conclusion

As the usages of IoT devices are increasing drastically one must be more alert about using the technologies. As the blockchain becomes part of IoT, it becomes difficult for a hacker to intrude into the blockchain network. Because the blockchain is a huge network and it is impossible for a person to capture the whole network. In the daily logs and transactions the hashing plays an important role, through the usage of Louvain clustering algorithm it is clearly analyzed that blockchain makes the IoT concept more reliable. In Louvain clustering algorithm the plotting is performed by giving both the x axis and y axis which makes a person easier to go through the graph.

10 References

[1] Haber, Stuart, and W. Scott Stornetta. "How to time-stamp a digital document." Conference on the Theory and Application of Cryptography. Springer, Berlin, Heidelberg, 1990.

[2] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." 2008.

[3] Alphand, Olivier, et al. "IoTChain: A blockchain security architecture for the Internet of Things." Wireless Communications and Networking Conference (WCNC), 2018 IEEE. IEEE, 2018.

[4] Singh, Parbhakar, Parveen Kumar, and Tanweer Alam. "Generating Different Mobility Scenarios in Ad Hoc Networks.", International Journal of Electronics Communication and Computer Technology, 4(2), 2014

[5] Sharma, Abhilash, Tanweer Alam, and Dimpi Srivastava. "Ad Hoc Network Architecture Based on Mobile Ipv6 Development." Advances in Computer Vision and Information Technology, 2008: 224.

[6] Alam, Tanweer. "Fuzzy control based mobility framework for evaluating mobility models in MANET of smart devices." ARPN Journal of Engineering and Applied Sciences 12, no. 15, 2017: 4526-4538.

[7] S. K. Usha Nandini Raghavan, Reka Albert, “Near linear time algorithm to detect community structures in large-scale networks,” CoRR, vol. abs/0709.2938, 2007.

[8] S. Fortunato and A. Lancichinetti, “Community detection algorithms: a comparative analysis,” in 4th International ICST Conference on Performance Evaluation Methodologies and Tools, 2009.

[9] S. Arifuzzaman, M. Khan, and M. Marathe, “A Spaceefficient Parallel Algorithm for Counting Exact Triangles in Massive Networks,” in 17th IEEE International Conference on High-Performance Computing and Communications, 2015.

Dr.Khaled Mofawiz Alfawaz is an Associate Professor at the Management Information Systems Department, Faculty of Economics and Administration, King Abdulaziz University, Jeddah, Saudi Arabia. He got a PhD from Brunel Business School, Brunel University, UK. He was Head of the Research and Development Center within the same Faculty. Formerly, he was Vice Dean of the English Language Institute at King Abdulaziz University. He was the Supervisor General for Quality Management at KAU and also of the Academic Accreditation Administration at the same university.