Distributed Authentication Using Blockchain for Protected Communication in Cloud Based IoT Platform

Ravi Kanth Motupalli [1*] & Krishna Prasad K. [2]

[1] Research Scholar, Institute of Computer Science & Information Sciences, Srinivas University, Mangalore, Karnataka, India and Assistant Professor, Department of CSE, VNR VJIET, Hyderabad, Telangana, India,
Orcid ID: 0000-0003-4893-5166; E-mail ID: ravikanth_m@vnrvjiet.in

[2] Associate Professor, Institute of Computer Science & Information Sciences, Srinivas University, Mangalore, Karnataka, India,
Orcid ID: 0000-0001-5282-9038; E-mail ID: krishnaprasadkcci@srinivasuniversity.edu.in

Area/Section: Computer Science.
Type of the Paper: Experimental Research.
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed in: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.7464623
Google Scholar Citation: IJMTS

How to Cite this Paper:
Motupalli, R. K., & Krishna Prasad, K., (2022). Distributed Authentication Using Blockchain for Protected Communication in Cloud Based IoT Platform. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, *7*(2), 669-678. DOI: https://doi.org/10.5281/zenodo.7464623

International Journal of Management, Technology, and Social Sciences (IJMTS)
A Refereed International Journal of Srinivas University, India.

CrossRef DOI: https://doi.org/10.47992/IJMTS.2581.6012.0244

Received on: 28/10/2022
Published on: 22/12/2022

Disclaimer: The scholarly papers as reviewed and published by the Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the SP. The SP disclaims of any harm or loss caused due to the published content to any party.

Distributed Authentication Using Blockchain for Protected Communication in Cloud Based IoT Platform

Ravi Kanth Motupalli [1]* & Krishna Prasad K. [2]

[1] Research Scholar, Institute of Computer Science & Information Sciences,
Srinivas University, Mangalore, Karnataka, India and Assistant Professor, Department of CSE, VNR VJIET, Hyderabad, Telangana, India,
Orcid ID: 0000-0003-4893-5166; E-mal ID: ravikanth_m@vnrvjiet.in

[2] Associate Professor, Institute of Computer Science & Information Sciences,
Srinivas University, Mangalore, Karnataka, India,
Orcid ID: 0000-0001-5282-9038; E-mail ID: krishnaprasadkcci@srinivasuniversity.edu.in

ABSTRACT

Purpose: *The technology has improvised to control the devices from the remote location using the IoT framework. To improvise the storage efficiency of the technology the IoT is integrated with the cloud network. When the huge size of the data is generated this cloud server hosts the space for the big data. But the secure exchange of the data between the IoT data is not efficient to protect the confidentiality of the data. The existing security systems are either concentrating on the authentication or secure validation. Hence there is a demand for the lightweight, less complex, and strong secure framework.*

Design/ Methodology/Approach: *The authentication phase of the proposed framework is designed using distributed block chain protocol to authenticate multiple users in the cloud environment. The SALSA20 encryption algorithm which augments the strength of the data security. The protected key exchange is done using the ReDH algorithm. Indexing is done using the hash algorithm to obtain the accuracy in the search results and to minimize the encrypting and decrypting time.*

Findings/ Results: *The proposed distributed block chain authentication framework is proved to be efficient with less encrypting and decrypting periods of about 0.25ms and 0.2ms respectively. 97.5% of the storage efficiency proves this model to be suitable for the cloud application.*

Originality/Value: *The proposed model has a dedicated database for the registration for the users and IoT devices which is used to validate the authentication of the system. The encryption is done using the SALSA20 algorithm and sensitivity level prediction process to measure the sensitivity score.*

Paper Type: *Experimental Research*

Keywords: Block chain codes, Cloud environment, IoT devices, SALSA20 encryption, Hash function, ReDH algorithm.

1. INTRODUCTION :

Internet of Things (IoT) is an evolving and thriving technology that authorizes data sharing across numerous small devices where the input is limited to access [1]. This technology has reached its peak through exponential growth in the past two decades. It was stated that around the year 2019 there was about 7600 million active IoT devices which is estimated to grow up to 24 billion in the next decade [2]. The growth rate of this technology is approximated to about 11% per annum. The growth of the IoT in the past two decades was illustrated in the Fig.1, where it is very clear that each year the number of IoT installations increases exponentially and drastically. The sudden growth of the IoT usage was happened in the year 2010 due to the evolution of the sensors at the very cheap cost where the sensors was used almost in all the networking applications.

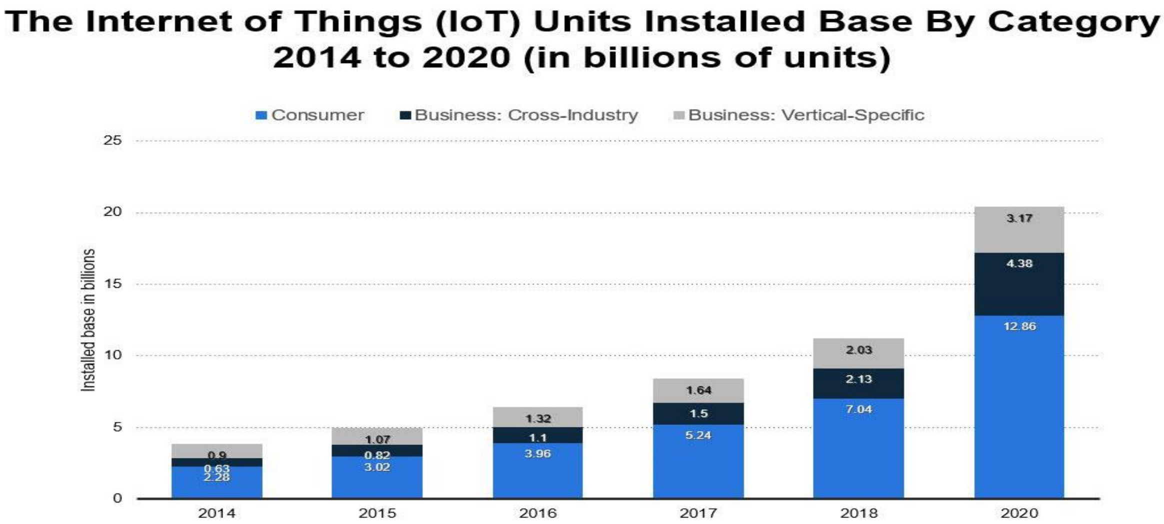

Fig. 1: Growth of IoT in the past two decades (Source: Forbes, 2018) [3]

IoT has its presence in many important applications as explained as follows. Wearable sensors is an extraordinary technology that was helpful in monitoring and tracking the health records of the patients from remote location. Smart city IoT is a contemporary application where the renovation, growth and maintenance of the city is tracked and executed through the devices connected to internet. IoT application in the smart home is an innovative feature that controls household gadgets and devices through sensors.

IoT devices are also used in agricultural applications to predict the climate, controlling the motor pumps and water outlets through devices connected through internet. Thus, through the sensors and the devices connected through the internet are used in many other applications like a retail business, tracking and monitoring systems, Industrial applications, etc [4].

Big Data from these IoT devices helps in the data refining, assessing and storage of the data [5]. When the analysis of the Big data is done enormous amount of space is required for the storage of the processed data. This flexibility of the expanding data storage during the analysis of the big data is resolved by the cloud computation [6]. Cloud computing simplifies the accessibility and authentication of data through remote devices [7]. This phenomenon influenced the researchers to develop an integrated authentication model for the secure data communication [8]. The generic IoT network framework is shown in the Fig.2. From the figure it is observed that the resource constrained devices are in the remote location and the server controlling the devices is in the cloud. Both are connected through the Internet.

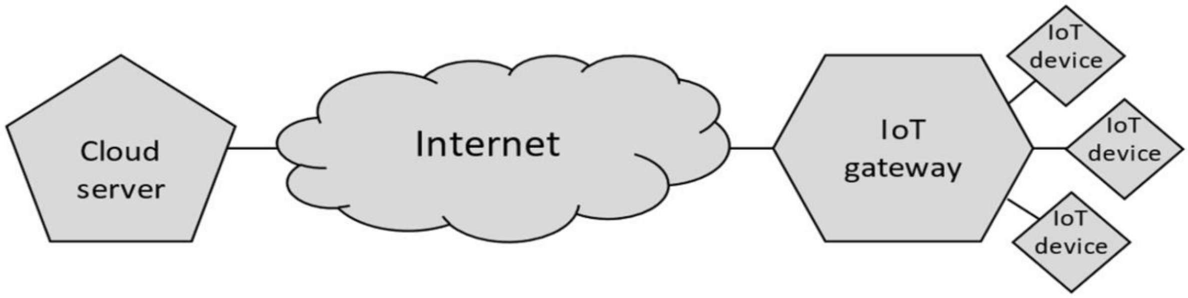

Fig. 2: Generic IoT Framework (Source: Author)

The end devices are used to interact with the required remote environment, IoT Gateway is used to collect the information and exchanges with the cloud server. An IoT gateway is a centralized hub that connects IoT devices and sensors to cloud-based computing and data processing. Modern IoT gateways often allow bidirectional data flow between the cloud and IoT devices. The cloud server uses cloud computation to analyze and process the collected information. A cloud server is a pooled, centralized server resource that is hosted and delivered over a network—typically the Internet—and accessed on demand by multiple users. Cloud servers can perform all the same functions of a traditional physical server, delivering processing power, storage, and applications. This simplifies and solves the issue of giant data storage requirement of the Big data. Though this integrated framework has many benefits, the security of the data exchange is still a weak structure. When handling the enormous data exchange, excellent security is a most demanded attribute to assure the safe transaction of the data [9].

2. LITERATURE REVIEW :

The framework of the cloud and IoT integrated structure was illustrated in the Fig.3. With the development of different networks and communication technologies the security of data sharing has become an explicitly significant factor in every communication [10]. Though there were numerous advantages in the IoT technologies, this also has some challenging issues like security and privacy [11]. These issues were considered as the significant and important attributes in the IoT communication. In recent days remote medical consultation through the modern gadgets and technologies has been very common and more helpful in the pandemic chaos [12]. This technology has many benefits including reduced medical expenses and improved quality of service [13]. But the patient’s details are required to be very confidential despite of the consultation platform.

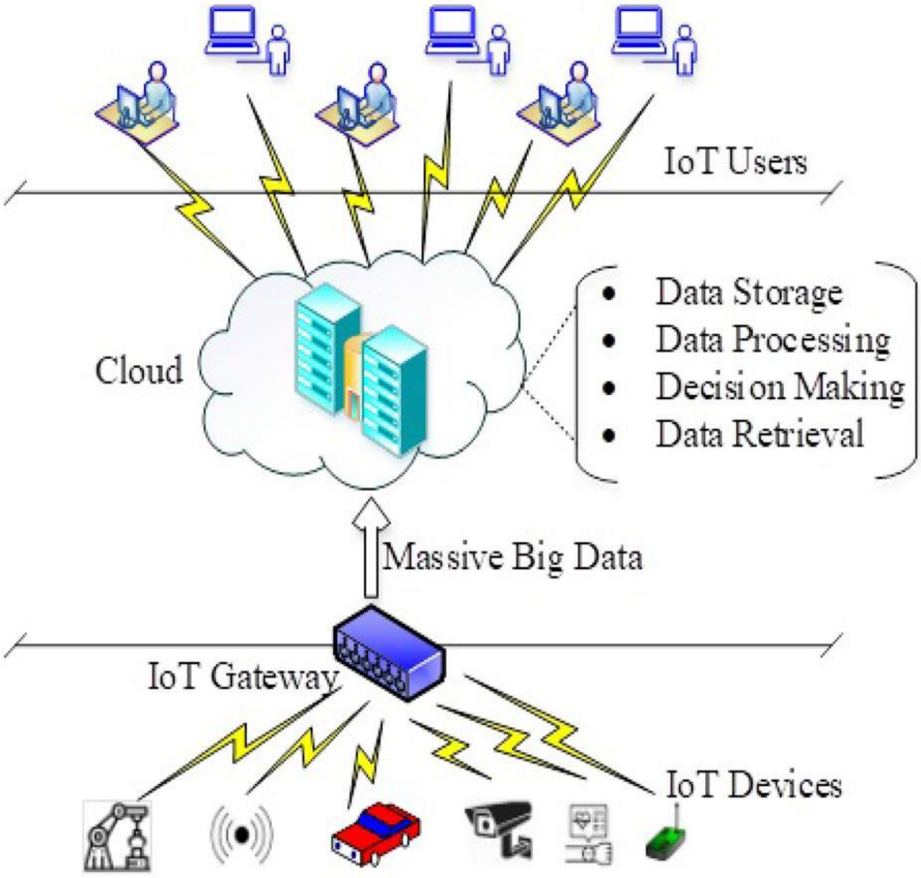

Fig. 3: Cloud integrated IoT Framework [14]

Though the IoT has its successful establishment in other sectors it is highly unlikely in Industrial application due to its security issues. This can be easily explained with the Philips-Hue attack [15]. In this attack in a smart city application, remotely programmed Light sources were re-programmed to turn on simultaneously causing a hike in the energy consumption leading turning off all the lights leaving the entire city in darkness. This illustrates the collapse is caused due to the poor security of the IoT network. This concerned the researchers to develop a safe model for the effective and protected communication in the IoT framework. The effective protected communication should be developed without compromising the quality of service. The requirement is to develop a framework to accomplish the privacy, probity, and the availability of the IoT service with advanced tools and security protocols.

Table 1: Literature survey on cloud security model

	Focus/ Constructs	Reference
Literature survey on cloud security model	An online authentication framework was proposed, where the online finger prints are used to secure the private data. The online fingerprint was recognisable by different servers to authenticate from multiple servers. But this method failed to avail strong security to preserve the confidential data than the actual bio metric data. As the online finger print can be duplicated easily this is an inefficient framework.	Zhu H, et al (2019). [16]
	To overcome the inefficiency in the Zhu et al proposal, an integrated security framework was suggested to combine the user ID and password. Fuzzy extractor is used to authenticate the user through Elgamal algorithm.The algorithm encrypts the user detail and the fuzzy extractor is used to obtain the online fingerprint details. As this framework has increased computational complexity this is not efficient for the Cloud-IoT applications	Maitra, T et al (2019). [17]
	A lightweight protocol using a smart card technique was developed. The major pitfall in this technique is that when the smart card is lost the security is not guaranteed.	Zhou L, et al (2019). [18]
	A block chain code-based security structure was proposed for information exchange with excellent hidden policy. But yet the authentication control in poor and is computationally complex.	Hao J, et al (2019) [19]
	The protected data recovery was done by indexing and key transaction protocols. In the data recovery phase the encryption was done through dual encryption technique. The keywords in the encrypted data were authenticated through fine grain encryption technique. The data encryption was done through AES protocol	An X, et al (2016). [20]
	A Retrieval Feature (RF) tree algorithm was proposed in the data recovery phase. In order to augment the indexing efficiency, RF tree was constructed. This tree was constructed based on a iteration protocol. Hence the searching period was extended due to repeated iteration.	Fu JS et al (2018). [21]
	Parameter based light weight decrypting protocol was developed for multiple servers.	Long J, et al (2019). [22]
	A three-factor authentication system was proposed, later which was discovered for a pitfall of decreased privacy.	Banerjee S, et al (2019). [23]

2.1. Security Challenges in the Cloud Integrated IOT Framework:

The challenges faced during the development of the security model are listed as follows.

- When the security provisioning id done centrally the vulnerability of the server is increased leading to the weakest network which can be hacked easily by tapping a single server.
- As the cloud can be able to accommodate n number of users simultaneously it is un-scalable and vast. But the existing security mechanisms are constrained with the resources and number of users. Hence a secured protocol irrespective of the number of users should be developed.
- With the analysis of huge data high power is consumed leading to the reduced performance characteristics. Hence a rapid and light weight security protocol should be developed to augment the performance of the system.

Thus, from the literature survey listed in the Table.1, it is clear that there is demand for novel secure mechanisms for cloud integrated IoT framework. The D-Block Security framework proposed in this study confides all the three phases like authentication, encryption, and decryption in a protected manner. Verification of the user and the end IoT devices is done to assure the efficient security of the information exchange. Only authorized users are able to recover and decrypt the encrypted data. The framework of the proposed architecture is explained in the following sections.

3. OBJECTIVES :

In order to develop an effective light weight protocol with improvised performance efficiency distributed authentication is used in combination along with the block chain codes. In this research distributed block security (DBlock Security) Scheme is proposed which has command over the protection, verification, encryption, and decryption of the data. The objective of this study is listed as follows,

(1) Analyzing the existing model of the loud security network and identifying the challenges in the model.
(2) To develop a distributed lightweight framework with augmented performance efficiency.
(3) Reducing or minimizing the data leakage in the data exchange system through an efficient protocol.

4. PROPOSED D-BLOCK SECURITY FRAMEWORK :

The proposed phase model of the Distributed block security framework is illustrated in the Fig.4.

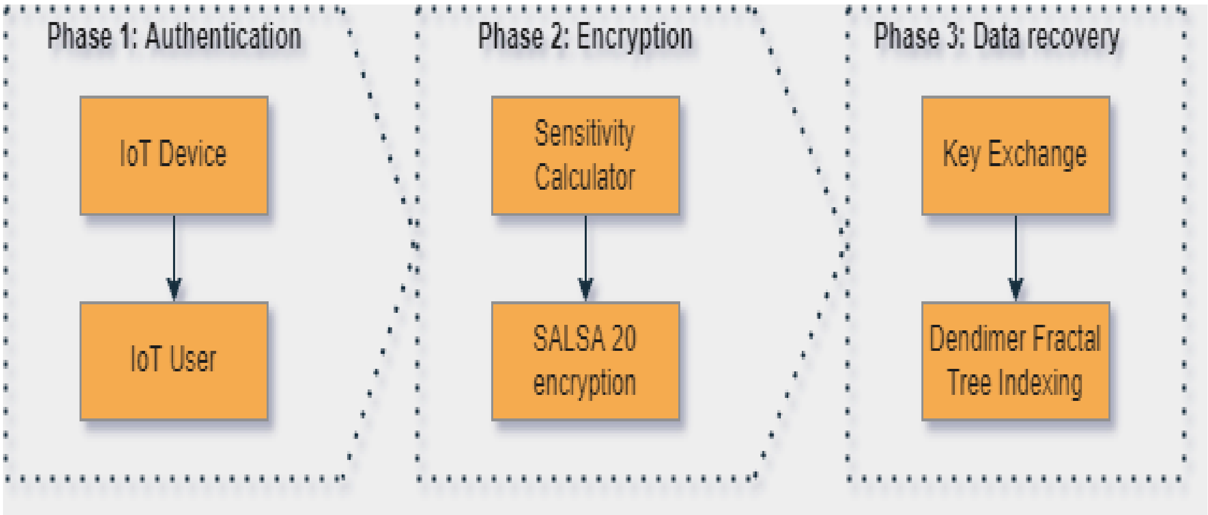

Fig. 4: Block diagram of Distributed block security framework (Source: Author)

The end IoT devices are the source for the generation of huge amount of information that is exchanged over the network. This information has to be stored in the cloud environment which is integrated with the spark technology to facilitate the large amount of data storage in the cloud servers. The proposed model confines to three different phases like verification, data encryption and data recovery. The primary concern of the proposed framework is to provide a strong security model for the data exchange between IoT devices and the cloud servers.
The first stage of the D-Block model is the verification of the End IoT devices. A novel database model is developed to verify both the user and the devices. For this purpose, the details has to be registered with the database. This process was a distributed and less complex process simplifying the complexity of the operation. Streebog hash algorithm is used for the registration of the details. These details are stored using the blockchain codes which augments the security level of the framework. The hash algorithm is used to produce the random hash values as the compression function. This is authenticated for the verification of the registered user and the end device and to block the unauthenticated users and devices. The second stage of the framework involves the encryption of the data. Salsa20 encryption algorithm is used for effective encryption in both rapid and simple manner. During encryption the data is divided into blocks and encrypted. For this the sensitivity of the data is measured to obtain sensitivity score. With the improved speed the optimal amount of energy is used thereby reducing the excessive power consumption for the huge amount of data.
The third phase of the framework involves the data recovery. The data recovery is done by indexing and searching. Through these methods the data is recovered in the form of cipher text. Then the ReDh decryption algorithm is used for the data retrieval through a protected key exchange. The entire process is simulated using the Phython simulator. Cloud network is set through Apache Spark 2.2.0. After configuring the required hardware the experiment is done. The data generated from the IoT devices are stored in the hadoop blocks. The proposed model is qualified for the big data applications. The encryption is done in the block chain codes ratehr than the servers so as to assure the security for the hidden key exchange.

5. RESEARCH METHODOLOGY :

In the Proposed model the encryption algorithm SALSA20 is considered as a expandable stream of ciphers, where the 256 bit keys of the ciphers are identified with 264 random streams with 64bytes

blocks. These blocks are seperated as 16 words which are inputted with 320 variables where each varaible is modified with one word. The permutated inputs are then formed into a complete 16 bit output which is added to the original 64 byte block of the SALSA20 algorithm. Thus each permutation is computationally formulated as the XOR function of each word in the rotated format with constant distance. The algorithm is designed to iterate up to 10 times with a series of 2 rounds. Each round id formulated to have 4 quarter round pipelines simultaneously. Thus in each quarter round modification of 4 words is programmed. The mathematical formulation of the SALSA20 algorithm is explained as follows,
Step 1: Initiate the encryption
Step 2: Set second order low level function for 10 double rounds
Step 3: Two 4 byte words are selected and the function S = x+y $|2^{32}|$ is performed
Step 4: Then X (xor) Y is done where bit by bit comparison is performed.
Step 5: Now the leftward rotation is done using the function 2^{x} S $|2^{32}\text{-}1|$
Step 6: Then the quarter round modification is done which is a reversible function
Step 7: Finally rowround function is performed and the resulting 16 words are given to square matrix.
Step 8: End the encryption

6. RESULTS AND DISCUSSION :

The results from the proposed model are then compared against the other models like Block AES [24], ABE [25] and Inverted Index[26] framework. The other frameworks consider either authentication process or secure validation, whereas the proposed model is designed based on both attributes.

6.1. Encryption Time:

The time required for encrypting the data is considered to be the most important analysis parameter. This attribute is decided based on the size of the data and the key. The size of the data directly represents the amount of information generated from the IoT devices. The amount of time taken by each algorithm for the encryption of the original data into cipher texts are 20.20ms, 25.85ms, and 0.25ms for the Block AES, ABE and D-Block algorithms respectively. From the results it is clear that the proposed model has minimal encryption time thereby reducing the time and computational complexity of the framework. The comparative analysis of the time taken to encrypt using different framework is shown in the Fig. 5.

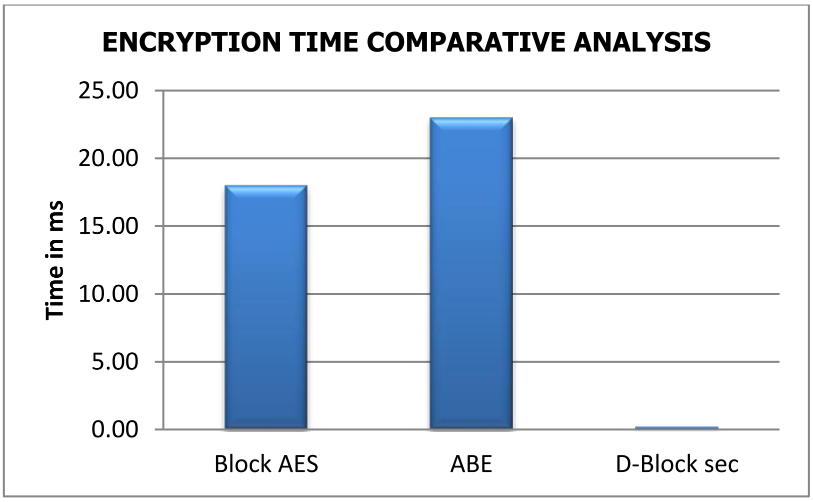

Fig. 5: Comparative Analysis of the Encryption time (Source: Author)

6.2. Decryption Time

The time required to decrypt the cipher text into original data is termed as the decryption time. Similar to encryption decryption also processed in blocks and is done simultaneously so as to decrease the time complexity of the framework. The obtained decryption time for the proposed algorithm, Block AES and ABE algorithms are 0.2 ms, 18ms and 23ms respectively. The graphical representation of the obtained data is given in the Fig.6. From the results it is evident that the proposed algorithm has less decryption time thereby increasing the performance of the proposed algorithm.

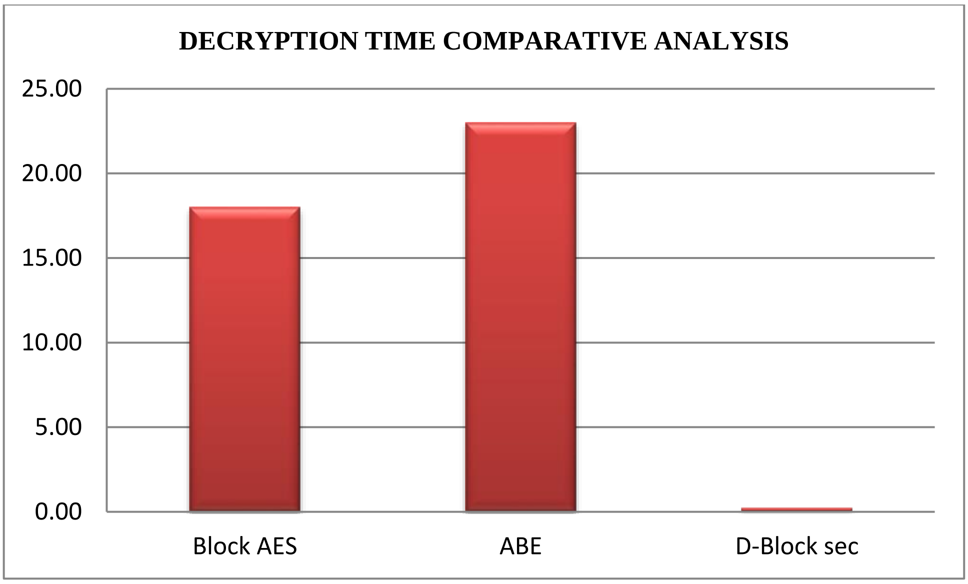

Fig. 6: Comparative Analysis of the Decryption time (Source: Author)

6.3. Storage

The storage efficiency of the proposed model is improvised when combined with the cloud computation. The storage efficiency in the proposed model is about 97.5%, where almost all the data is analyzed without any error or deviation. The indexing was accurate up to 98% which makes the search easier for the data retrieval. Where the storage efficiency for the Block AES and ABE was 50% and 60% respectively. Thus from the results it is declared that the proposed model is suitable for big data integrated with the cloud technology.

7. CONCLUSION :

Thus, from the obtained results it is very clear that the proposed model is not only simple and less complex but also efficient in securing the information exchange between the IoT devices in the cloud environment. The cloud environment is integrated with the spark, which makes it suitable for the limited resource framework. The developed framework augments the security by validating the registered user in the dedicated database. This framework is flexible and is less complex. The future work of this study may be scheduled to analyse the steps to verify the user profile during registration to further improvise the efficiency of the designed framework.

REFERENCES :

[1] Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University-Computer and Information Sciences, 30*(3), 291–319. Google Scholar↗ DOI↗

[2] Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. *Journal of Electrical and Computer Engineering, 1*(1), 1–26. Google Scholar↗ DOI↗

[3] Louis Columbus, (2018). 10 Charts That Will Challenge Your Perspective Of IoT's Growth https://blogs-images.forbes.com/louiscolumbus/files/2018/06/The-Internet-of-Things-IoT-Units-Installed-Base-By-Category-2014-to-2020-in-billions-of-units.jpg

[4] Narayanan, U., Paul, V., & Joseph, S. (2017, August). Different analytical techniques for big data analysis: A review. In *2017 International conference on energy, communication, data analytics and soft computing (ICECDS)* (pp. 372-382). IEEE. Google Scholar↗ DOI↗

[5] Unnikrishnan, A., Narayanan, U., & Joseph, S. (2017, August). Performance analysis of various supervised algorithms on big data. In *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)* (pp. 2293-2298). IEEE. Google Scholar↗ DOI↗

[6] Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. *Future Generation Computer Systems*, *79*(1), 849-861. Google Scholar↗ DOI↗

[7] Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big Data and cloud computing: innovation opportunities and challenges. *International Journal of Digital Earth*, *10*(1), 13-53. Google Scholar↗ DOI↗

[8] Delsing, J. (2017). Local cloud internet of things automation: Technology and business model features of distributed internet of things automation solutions. *IEEE Industrial Electronics Magazine*, *11*(4), 8-21. Google Scholar↗ DOI↗

[9] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*(1), 10-28. Google Scholar↗ DOI↗

[10] Gutub, A., & Al-Ghamdi, M. (2020). Hiding shares by multimedia image steganography for optimized counting-based secret sharing. *Multimedia Tools and Applications*, *79*(11), 7951-7985. Google Scholar↗ DOI↗

[11] Leloglu, E. (2016). A review of security concerns in Internet of Things. *Journal of Computer and Communications*, *5*(1), 121-136. Google Scholar↗ DOI↗

[12] Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer networks*, *148*(1), 283-294. Google Scholar↗ DOI↗

[13] Alassaf N, Alkazemi B, Gutub A, (2017). Applicable light-weight cryptography to secure medical data in IOT systems. *Journal of Research in Engineering and Applied Sciences*, *2*(2), 50–58. Google Scholar↗

[14] Narayanan, U., Paul, V., & Joseph, S. (2022). Decentralized blockchain based authentication for secure data sharing in Cloud-IoT. *Journal of Ambient Intelligence and Humanized Computing*, *13*(2), 769-787. Google Scholar ↗ DOI↗

[15] Ronen, E., Shamir, A., Weingarten, A. O., & O'Flynn, C. (2017, May). IoT goes nuclear: Creating a ZigBee chain reaction. In *2017 IEEE Symposium on Security and Privacy (SP)* (pp. 195-212). IEEE. Google Scholar↗ DOI↗

[16] Zhu, H., Yuan, Y., Chen, Y., Zha, Y., Xi, W., Jia, B., & Xin, Y. (2019). A secure and efficient data integrity verification scheme for cloud-IoT based on short signature. *IEEE Access*, *7*(1), 90036-90044. Google Scholar↗ DOI↗

[17] Maitra, T., Obaidat, M. S., Giri, D., Dutta, S., & Dahal, K. (2019). ElGamal cryptosystem-based secure authentication system for cloud-based IoT applications. *IET Networks*, *8*(5), 289-298. Google Scholar↗ DOI↗

[18] Zhou, L., Li, X., Yeh, K. H., Su, C., & Chiu, W. (2019). Lightweight IoT-based authentication scheme in cloud computing circumstance. *Future Generation Computer Systems*, *91*(1), 244-251. Google Scholar↗ DOI↗

[19] Hao, J., Huang, C., Ni, J., Rong, H., Xian, M., & Shen, X. S. (2019). Fine-grained data access control with attribute-hiding policy for cloud-based IoT. *Computer Networks*, *153*(1), 1-10. Google Scholar↗ DOI↗

[20] Wang, X. A., Xhafa, F., Cai, W., Ma, J., & Wei, F. (2016). Efficient privacy preserving predicate encryption with fine-grained searchable capability for Cloud storage. *Computers & Electrical Engineering*, *56*(1), 871-883. Google Scholar↗ DOI↗

[21] Fu, J. S., Liu, Y., Chao, H. C., Bhargava, B. K., & Zhang, Z. J. (2018). Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing. *IEEE Transactions on Industrial Informatics*, *14*(10), 4519-4528. Google Scholar↗ DOI↗

[22] Long, J., Zhang, K., Wang, X., & Dai, H. N. (2019, July). Lightweight distributed attribute based keyword search system for internet of things. In *International Conference on Security, Privacy*

and Anonymity in Computation, Communication and Storage (pp. 253-264). Springer, Cham. Google Scholar↗ DOI↗

[23] Banerjee, S., Odelu, V., Das, A. K., Srinivas, J., Kumar, N., Chattopadhyay, S., & Choo, K. K. R. (2019). A provably secure and lightweight anonymous user authenticated session key exchange scheme for Internet of Things deployment. *IEEE Internet of Things Journal*, *6*(5), 8739-8752. Google Scholar↗ DOI↗

[24] Li, J., Zhang, Y., Chen, X., & Xiang, Y. (2018). Secure attribute-based data sharing for resource-limited users in cloud computing. *Computers & Security*, *72*(1), 1-12. Google Scholar↗ DOI↗

[25] Lin, C., He, D., Huang, X., Choo, K. K. R., & Vasilakos, A. V. (2018). BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. *Journal of network and computer applications*, *116*(1), 42-52. Google Scholar↗ DOI↗

[26] Shen, M., Ma, B., Zhu, L., Du, X., & Xu, K. (2018). Secure phrase search for intelligent processing of encrypted data in cloud-based IoT. *IEEE Internet of Things Journal*, *6*(2), 1998-2008. Google Scholar↗ DOI↗

****