computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

SECURING CLOUD DATA AGAINST CYBER-ATTACKS USING HYBRID AES WITH MHT ALGORITHM

Jayapandian N

Faculty of Engineering, CHRIST (Deemed to be University), India, njayapandian@gmail.com

Paper history:
Received 18 May 2020
Received in revised form 27 September 2020
Accepted 17 October 2020
Available online 30 December 2020

Keywords:
AES Algorithm;
Big data;
Cloud computing;
Data Security;
Data Storage;
MHT Algorithm.

Abstract: Cloud computing is dealing with large amount of data during data communication. This data processing is named as big data. The big data is growth of the demand in accessing the storage, computation and communication. This big data has the major defects. A raising issue in emerging big data is cost minimization. The architecture of big data ranges over multiple machines and cluster which have sub system. The major challenge of this big data is pre-processing and analysing the data patterns. This research article is dealing with different data pre-processing and secure data storage. There are many research challenges during this data process. The possible gap and drawbacks in the technology are identified through this survey and the efficient big data service is provided through MHT and AES algorithm. The main aim of this proposed method is to provide better data security during larger data process. The proposed hybrid MHT with AES algorithm is to minimize the encryption and decryption time apart from that it reduces the attacker ratio. All these parameters automatically increase the Quality of Service.

1. INTRODUCTION

Big data refers to the progressing of huge data at high speed, making it difficult to manage such massive amount of data. The big data has three main characteristic that is V cube. Primary characteristic is volume of data. Secondary characteristic is variety of data, apart from this velocity of data is also measured. This big data concept is implemented on different levels of applications. The network performance is measured during data communication. The recent business forecasting trend analysis is also used. The history said that the world has been facing the big data challenges in the last four decades. In 1970 the big refers to megabytes overtime, the big grew to gigabytes then it moves to terabytes but now it is in petabytes also it may grow to exabytes as the volume of the data is very large. Now Hadoop and HDFS becomes the prominent platform for handling in larger data with web circles. This model has to present low level map reducing programming model which was chosen instead of high level declarative language and framework which allows the data analyses to be exposed much easier to write and debug. The process of studying and grasping the characteristic of large set of data by taking out the geometrical and statistical pattern is known as data analytics. The above mentioned characteristics of data set increases the complicity of data. Cloud Computing is a technology used to perform efficient computation by using the centralized storage, memory, processing and bandwidth facilities. Data and applications are maintained with the help of internet and central remote server. The loss of data and software are the most demanding aspects of cloud. There are different sources which may damage the system like computer viruses, computer hacking, it becomes more common. The major security refers the cloud computing as it comprises a lot of technologies including networks, virtualisation, operating system, resource scheduling transaction management and load balancing and memory management. In future Cloud and IOT are interlinked to solve data security problem [1]. The cloud data security problem is also

This paper has been submitted for the Open Special Issue on Green Mobile Computing and IoT Systems. Assessment, Modeling, Assurance.

solved by using traditional fingerprint technology [2]. The latest deployment of cloud infrastructure is to provide higher weightage in storage and security. The analytic platforms are more frequently cited in the networking. The last big trends, server and storage virtualization was all about workload on hardware. In early days the basic networking system was used by several organizations even though they need certain latency requirements because they need to spend a lot of money to update. Big data requires full rip and replacement of legacy network infrastructure, many organizations choose green field with the support of Hadoop big data [3].

2. STATE OF THE ART

The big data and cloud computing are two pillars of the same building. The main objective of big data is improving the computational performance during cloud storage. The feature of cloud is to provide bulk usage of data over various computers and to store data of large size which leads to the big data applications. The concept of distributed data storage is dealing with this big data problem. The primary technology of cloud computing is managing the architecture of network protocol and big data is analysis of the business perspective. Big data does not focus on the end user but cloud computing purely focuses on the end user. This property shows the big data as a unique in comparison with other concepts. Cloud computing handles larger data resources in world, all these resources are monitored in secure way [4]. The data storage is major problem in online cloud storage; the hybrid iMLEwCE algorithm provides better solution for this kind of problem [5]. The process of creating the virtual structure for big data system is known to be big data virtualization. It enables the user to use data assets. To handle the big data analytics the big data virtualization tool is called. In general big data performance should be measured on some indexing techniques; these can be real time index methods [6]. The complex system is represented for heterogeneous and distributed system is the main idea of virtualization through specific interfaces like hardware and data storage design with virtual components. Main advantage of using cloud and big data is to minimize the cost and increase the service capacity creating larger storage space [7]. Both big data and cloud computing is working with the help of virtualization concept. Cloud computing should be hosted in cloud data centers; it will handle millions of data and communication utilization to produce carbon emission [8]. The modern cloud based smart device is also facing security threats [9]. Five major reasons why we move from cloud to big data: in the cloud system we cannot manage the data in a better way but in the big data you will manage the data better than in a cloud. You will get more benefit of speed and capacity than cloud. End user can visualize the data in big data and may also find new opportunity in big data. Your data analysis capability will evolve in big data. Fig. 1 shows how the technology development has been explored in recent years. The data security problem is solved by either symmetric or asymmetric encryption algorithm [10].

Figure 1 – Technological Development

3. PROBLEM STATEMENT

The major research problem of big data is simplified into two levels. First one is engineering perspective; this should focus on data base management and measurement of the storage performance. Second one is semantic; this is the process of taking out the synonym of the information from the unstructured data in massive volume. The jet propulsion laboratory has found some major challenges of the big data. Larger data volume is dealing with low power architecture [11]. While designing a system the power that needs for processing the data and the power which requires for cooling the processing system should be considered together. This kind of big data is analyzed by using different machine learning algorithms. This data process is handled with data mining technique to separate the data patterns [12]. This segregation is processed into two categories, that is, conventional and non-conventional data. The network congestion may be caused when we send all data with high sampling rate. In the real time data processing all the data is processed that means storing in cloud and network latency problem should raise [13]. That network latency is affecting the communication during data storage. Avoiding this kind of problem they establish local server to store the data within that network, then that data automatically updates the cloud server within some time interval [14]. This cloud storage and big data process face huge security and privacy issue during the cloud communication. This cloud data security problem is

also solved by using hybrid probabilistic and homomorphic encryption algorithm [15]. The dynamic data storage is most challenging task comparing to other problems. The major goal of big data security is providing higher security in sensitive data with an existing method. This existing technology is providing security protection in static data storage, but modern storage technology is dynamic. This dynamic data storage is very hard in comparison to traditional method. The problem of this dynamic method is different type of data processed with the same time. Apart from this some legal issues also arise in this cloud data storage, some sensitive data is not allowed to share third party server. But this cloud technology always depends on the third party server. The traditional query method is executed very fast but security is a major issue. The big data query processes higher volume of data. This data velocity is also measured in dynamic system. Here they use approximate result prediction. This method is to predict the accurate results. This larger volume of data is handled with data analytics algorithm. There are two major components used; efficient resource and power consumption of that data process. The computational power is important parameter. To handle larger data set in a particular time computational power is reduced, that is the reason that some computing algorithm is used to solve this problem. The social media and web analysis system is generating huge volume of data [16]. In social media they use more big data technology to reduce the storage space in communication server. They maintain the relationship of real world data with big data query [17]. The next problem of this big data is query optimization, because for the purpose of handling large volume of data they use large query. This query is also taking more space during this data process [18]. To avoid this problem query optimization is also needed [19]. Energy consuming, necessary memories, operating time, essential storage are some of the perspectives that have to be considered during the optimization process [20]. The key in query processing in cloud is the parallel processing [21]. In service level agreement concept deals with the multi-tenant data process unit [22]. This multi-tenant means that multiple users can use this cloud computing technology in real time server [23]. That particular time design and development of server is also facing some challenge [24]. Apart from data theft today's cloud data communication arises many other issues. Account hijacking is one of the major issues, in the recent days many politicians' social media accounts were hijacked. In general cloud service is to be provided by third party service provider, during this service attackers take over the API. That means API keys are used between service accesses.

4. METHODOLOGY

To overcome the data theft by the hackers, encrypting process has been evolved. This encryption and decryption of data is done using two type of key namely, symmetric key algorithm and asymmetric algorithm. The difference between symmetric and asymmetric is that the same key is used both by sender and receiver and it is symmetric. When they use alternate key for sender and receiver, it is asymmetric encryption [25]. AES algorithm is an example of symmetric key algorithm [26].

4.1 AES ALGORITHM

This algorithm is working on 128 bits of data length and executes the loop Nr-1 times depending upon the key length. Add round key transformation is performed in the first loop and mix column transformation is carried out in the last loop. These transformations occur only in the first and the last loop and so these loops are different from any other loop.

Steps involved in AES algorithm:

Step 1: Expanding the key - The value of round key is resulting from the cipher value using Rijindal algorithm.
Step 2: First Operation
Round Key should add- ever state is joined the round key value using XOR Operation
Step3: Round Operation
Sub Bytes – This sub byte operation substitute nonlinear bytes with an existing.
Shift the Rows – The existing values are shifted in the round key value.
Mix Columns – The column mixed with in the parameter.
Add the Round Key
Step 4: Last Stage (Columns are not mixed)
Bytes Sub
Add Round Key

Then the decryption is working backward operation during data transmission. Then major component of AES algorithm is round key addition. This round key is added to the existing result and column is also mixed. In this operation every key value is derived from the main key. In general, encrypting and decrypting algorithm needs 128-bit round keys. The column is also mixed with other parameter; this polynomial multiplication is used for this operation.

4.2 MULTIPLE HYPOTHESIS TRACKING (MHT)

Reid was the first who proposed this multiple hypothesis tracking algorithm which is a fundamentals of multi-target tracking field. Usually MHT is used to track the targets in both two dimensional and three dimensional spaces. A set of hypotheses on various states are maintained by this algorithm in which each hypothesis has the message about the targets with their tracks. A new scan is received by the system which contains the data from the sensor which is also known as measurement. Those measurements are associated with an existing cluster or with a new cluster. An enormous hypothesis generated by this algorithm is bridled by pruning the hypothesis tree. Habitually the strategy of pruning includes limiting the number of leaves, depth of the tree. The hypotheses are always produce best result at the same execution time and system memory space is taking this hypothesis. In order to reduce the processing time clustering is used which divides the hypothesis tree into several trees between the tracks of target. Cluster splitting can be performed if non-intersecting sets of constraints are found. The multiple hypothesis library is used to implement the MHT algorithm which is described by Antunes et al. Clustering of these nodes is analyzing the tree depth and tree size. This measurement is dynamically executed. Then a new hypothesis is generated for each set of measurements associated with the same cluster, followed by cluster tree pruning. The clusters may be degraded according to the rules and if two tracks share a common measurement then they must be on the same cluster. The operations of the library are similar to the ones of the traditional MHT.

The proposed enhanced with the security framework that incorporates the various security preserving cryptographic techniques. In Fig. 2, in the model we have employed a two algorithm method namely AES and MHT to provide the secure environment in the big data. When there is enormous number of user accesses to the same server the rate of security and privacy level decreases.

Table 1 shows different abbreviations used in proposed model. In order to ignore such problem, AES and MHT algorithm is proposed with the big data. The flow represents the way how the data is processed in the big data server in which the data being accessed by the user is primarily stored in files and files are encrypted using AES and MHT algorithm. The encrypted data is then stored in the big data server. The main cause of this proposed system is to provide security and privacy over the data in the server.

Table 1. Abbreviations used in Proposed Model

Notations	Abbreviations
AES	Advanced Encryption Standard
MHT	Multiple Hypotheses Tracking
i	Iteration Hypothesis
iMLEwCE	interactive Message-Locked Encryption with Convergent Encryption

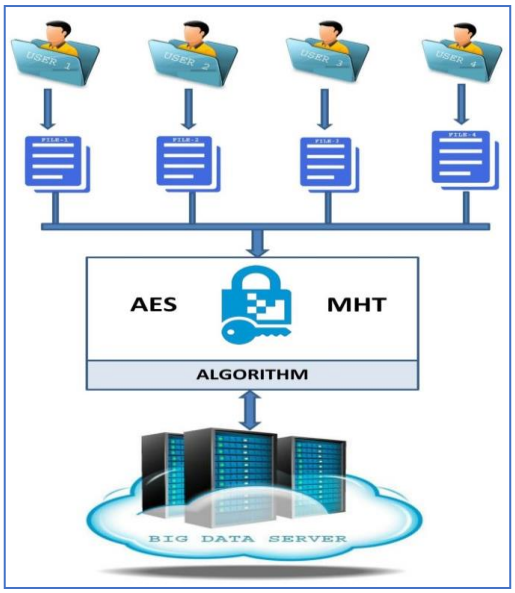

Figure 2 – Hybrid AES and MHT Algorithm

The first one is If i1 and i2 where generated at the same hypothesis generation, then they must remain in the same cluster. And the second rule is: If, to assert i1, one needs to know i2, then both must remain in the same cluster. Only one hypothesis in the MHT is concerned as an exact process which means only one hypothesis will survive pruning. The first rule illustrates that there is slice information in the hypothesis in each global hypothesis. Before the implementation of the second rule library will ensure the information about the application to be generated. The library provides the subset of information about the application when it creates the new hypothesis in the leaf. According to the second rule, the information provided by the library and the application must be kept on the same cluster. Thus the MHT algorithm provides better result than any other method which propagates one hypothesis but the advantages of performance on cost. This method is much more complicated in the implementation than other tracking methods as they have many processing steps. In addition to that each step can be implemented in a variety of ways. The cloud service provider normally provides the data encryption, and then they will provide the encryption key to the client. These keys are generally used for data decryption. In modern industry they use three different conditions. First one is to transfer

information that means moving or motion the data from one location to other location. Second condition is information rest, it is stored the data in one particular location is not used or transmitted. Final condition is real time data use; this condition is that data is not stored or transmitted. It is processed one application is transformed to other application, best example of this cloud data is IoT device data. Based on these condition encryption keys are used. In this proposed model I used the first condition; data is transmitting from server machine to client machine. Under this particular condition, AES algorithm is working both 128 and 256 bits but I am choosing 128 bit. Reason choosing 128 bit takes less encryption time compare to larger key size.

5. RESULT AND DISCUSSION

The proposed algorithm experimental result was carried out in Hadoop environment. The random input data is taken and executed. The performance evaluation is measured based on encryption time, decryption time and attackers ratio. Table 2 and Fig. 3 explain the encryption time of the hybrid algorithm that is advanced encryption standard and multiple hypotheses tracking algorithm. When these algorithms are used individually the encryption time will be increased. The encryption time of the algorithm is considered in milliseconds.

Table 2. Encryption Time Comparison

Input Data	AES (ms)	MHT (ms)	AES with MHT (ms)
Data set 1	529	685	436
Data set 2	652	457	329
Data set 3	324	667	410
Data set 4	826	537	380

Consider the data set 1 where the encryption time in the first algorithm (AES) is 529 milliseconds, the encryption time in second algorithm (MHT) is 685 milliseconds, but in the combined algorithm that is (AES with MHT) the encryption time is 436 milliseconds. Consider input size of data set 2 where the encryption time of the first algorithm (AES) is 652 milliseconds, in second algorithm (MHT) the encryption time is 457 milliseconds.

The Proposed algorithm (AES with MHT) is being combined to give the encryption time of 329 milliseconds. Consider data set 3 for input size. The algorithm 1 (AES) has the encryption time of 324 milliseconds, second algorithm (MHT) has the encryption time of 667 milliseconds. The hybrid algorithm (AES with MHT) has the encryption time of 410 milliseconds. Now consider the data set 4 where the encryption time of algorithm 1 is 826 milliseconds, the encryption time of the second algorithm is 537 milliseconds, hybrid algorithm gives the encryption time of 380 milliseconds. These examples of data set 1, data set 2, data set 3, data set 4 explain that when the algorithms were used individually the encryption time of the individual algorithm is high, but then these algorithms were compared to give low encryption time as compare to the encryption time of the individual algorithm.

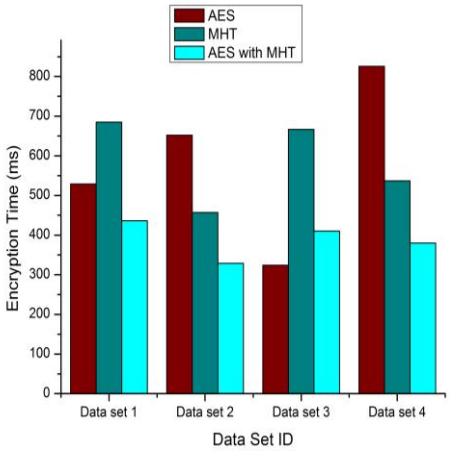

Figure 3 – Encryption Time Analysis

Table 3 and Fig. 4 explain the decryption time of the hybrid algorithm that is advanced encryption standard and multiple hypotheses tracking algorithm. When these algorithms are used individually the decryption time will be increased. The decryption time of the algorithm is considered in milliseconds. Consider the data set 1 where the decryption time in the first algorithm (AES) is 462 milliseconds.

Table 3. Decryption Time Comparison

Input Data	AES (ms)	MHT (ms)	AES with MHT (ms)
Data set 1	462	843	314
Data set 2	822	654	587
Data set 3	677	765	460
Data set 4	733	965	689

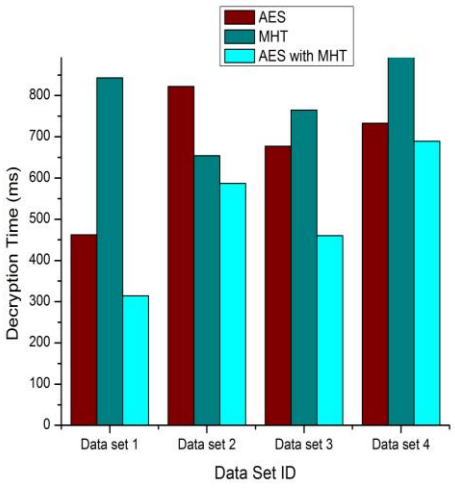

Figure 4 – Decryption Time Analysis

The decryption time in second algorithm (MHT) is 843 milliseconds, but in the combined algorithm

that is (AES with MHT) the decryption time is 314 milliseconds. Consider input size of data set 2 where the decryption time of the first algorithm (AES) is 822 milliseconds, in second algorithm (MHT) the decryption time is 654 milliseconds, when these algorithms (AES with MHT) are combined to give the decryption time of 587 milliseconds. Consider data set 3 for input size. The algorithm 1 (AES) has the decryption time of 677 milliseconds, second algorithm (MHT) has the decryption time of 765 milliseconds. The hybrid algorithm (AES with MHT) has the decryption time of 460 milliseconds. Now consider the data set 4 where the decryption time of algorithm 1 is 733 milliseconds, the decryption time of the second algorithm is 965 milliseconds, hybrid algorithm gives the decryption time of 689 milliseconds. These examples of data set explain that when the algorithms were used individually the decryption time of the individual algorithm is high, but when these algorithms are compared to give low decryption time as compare to the decryption time of the individual algorithm. Table 4 and Fig. 5 explain the execution time of the algorithms.

Table 4. Execution Time Comparison

Input Data	AES (ms)	MHT (ms)	AES with MHT (ms)
Data set 1	456	657	856
Data set 2	678	345	703
Data set 3	285	564	694
Data set 4	345	456	593

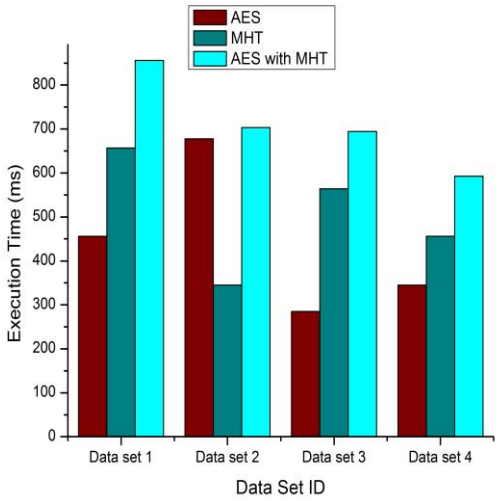

Figure 5 – Execution Time Analysis

When the algorithms were individually used the execution time of the algorithm was very low as compare to the hybrid algorithm. The input sizes are the data sets and the execution time are taken in milliseconds. The data set 1 where the execution time of first algorithm (AES) is 456 milliseconds. The second algorithm (MHT) gives the execution time of 657 milliseconds, but the hybrid algorithm (AES with MHT) gives the execution time of 856 milliseconds. Consider data set 2 where the execution time is 678 milliseconds for the (AES) first algorithm, second algorithm has the execution time of 345 milliseconds, but the combined algorithm (AES with MHT) gives the execution time of 703 milliseconds. Consider data set 3 in which the execution time for the (AES) first algorithm is 285 milliseconds, for the second algorithm(MHT) the execution time is 564 milliseconds, but the hybrid algorithm (AES with MHT)has the execution time of 694 milliseconds. Take the data set 4 where the execution time of the (AES) first algorithm is 345 milliseconds and the second algorithm (MHT) gives 456 milliseconds, but the hybrid algorithm (AES with MHT) gives the execution time of 593 milliseconds. The above explanations clearly show that the execution time of the individual algorithm is low when comparing to the hybrid algorithms.

Table 4 and Fig. 6 explain the data attacking ratio of the hybrid algorithm that is advanced encryption standard and multiple hypotheses tracking algorithm. When these algorithms are used individually the data attacking ratio is high. The attacker's ratio is generated based on the first level attack. This data is generated based on if hacker knows the encryption key, then we try to make an attack during transmission. For the simulation purposes randomly we try to attack the user's data. The proposed model attackers ratio provides better result.

Table 4. Attacker Ratio Comparison

Input Data	AES (%)	MHT (%)	AES with MHT (%)
Data set 1	43%	49%	20%
Data set 2	38%	62%	15%
Data set 3	30%	59%	24%
Data set 4	52%	61%	26%

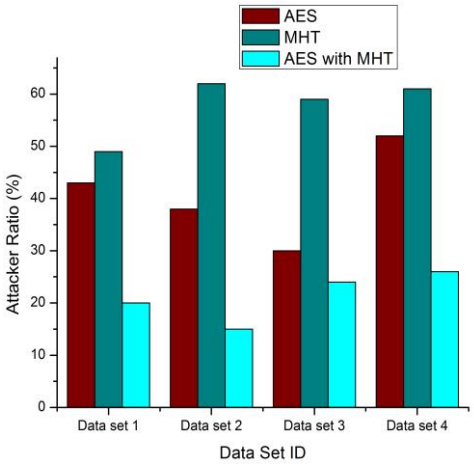

Figure 6 – Attackers Ratio Analysis

Consider the data set 1 where the data attacking ratio of the first algorithm (AES) is 43%, the second algorithm (MHT) has the data attacking ratio of 49%, but the combined algorithm (AES with MHT) gives the data attacking ratio of 20%. Consider the data set 2 in which the first algorithm (AES) gives the data attack ratio of 38% and the second algorithm (MHT) has the data attack ratio of 62% but the hybrid algorithm gives the data attack ratio of 15%. Take the data set 3 where the algorithm 1 (AES) has the data attack ratio of 30%, the data attack ratio of the second algorithm (MHT) is 59%, but the combined algorithm gives the data attack ratio of 24%. Consider data set 4 here the first algorithm (AES) gives the data attack ratio of 52%, the second algorithm (MHT) has the data attack ratio of 61%, but the combined algorithm gives the data attack ratio of 26%. The above explanations clearly gives the data attack ratio of the individual algorithm (AES or MHT) that has high data attack rate when these algorithms were being compared (AES with MHT) to give the low data attacking ratio.

6. CONCLUSION

This article presents the various merits and demerits of the big data. There are great opportunities as well as the challenges in both computation and data analysis. In the field of modern software architecture this big data technology is most wanted one. This technology is facing complex research problem in modern cloud data storage. The software industry collects and maintains huge volume of data in real time data processing. The MHT and AES algorithms are used to solve the security problems which are mentioned in the problem statement. The design of AES is implemented using APEX20KCFPGA. It basically provides higher quality and higher system performance. The system is known to be better in latency and also in throughputs. In this article the big data concept, Scope, and advantages and challenges have been discussed. Besides its critical issues of privacy and security in big data there are other problems that will be discussed in future. Even though the clear solution is not given exactly to the entire issue of big data and this discussion helps to framework the researchers.

7. REFERENCES

[1] A. Botta, W. de Donato,V. Persico, A. Pescapé, "Integration of cloud computing and internet of things: a survey," *Future Generation Computer Systems*, vol. 56, issue 3, pp. 684-700, 2016.

[2] N. Jayapandian, A. M. Z. Rahman, M. Koushikaa, S. Radhikadevi, "A novel approach to enhance multilevel security system using encryption with fingerprint in cloud," *Proceedings of the World IEEE Conference on Futuristic Trends in Research and Innovation for Social Welfare*, Coimbatore, India, Feb 29, 2015, pp. 1-5.

[3] A. Prakash, N. Navya, N. Jayapandian, "Big data preprocessing for modern world: Opportunities and challenges," *Proceedings of the International Conference on Intelligent Data Communication Technologies and Internet of Things*, India, August 7, 2018, pp. 335-343.

[4] G. Da Cunha Rodrigues, R.N. Calheiros, V.T. Guimaraes, G.L.D. Santos, M.B. De Carvalho, L.Z. Granville, L.M.R. Tarouco, R. Buyya, "Monitoring of cloud computing environments: concepts, solutions, trends, and future directions," in *Proceedings of the 31st Annual ACM Symposium on Applied Computing*, April 4, 2016, pp. 378-383.

[5] N. Jayapandian, A. M. J. Md Zubair Rahman, "Secure deduplication for cloud storage using interactive message-locked encryption with convergent encryption, to reduce storage space," *Brazilian Archives of Biology and Technology*, vol. 61, issue 1, pp. 1-13, 2018.

[6] A. Gani, A. Siddiqa, S. Shamshirband, F. Hanum, "A survey on indexing techniques for big data: taxonomy and performance evaluation," *Knowledge and information systems*, vol. 46, issue 2, pp. 241-284, 2016.

[7] M. N. Cheraghlou, A. Khadem-Zadeh, & M. Haghparast, "A survey of fault tolerance architecture in cloud computing," *Journal of Network and Computer Applications*, vol. 61, issue 1, pp. 81-92, 2016.

[8] J. Shuja, A. Gani, S. Shamshirband, R. W. Ahmad, & K. Bilal, "Sustainable cloud data centers: a survey of enabling techniques and technologies," *Renewable and Sustainable Energy Reviews*, vol. 62, issue 1, pp. 195-214, 2016.

[9] F. A. Alaba, M. Othman, I. A. T. Hashem, & F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10-28, 2017.

[10] M.B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, & Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," in *Proceedings of the* 2017 IEEE I*nternational conference on engineering and technology*, Antalya, Turkey, Aug 21, 2017, pp. 1-7.

[11] P. J. Stephenson, T. M. Brooks, S. H. Butchart, E. Fegraus, G. N. Geller, R. Hoft, L. McRae, "Priorities for big biodiversity data," *Frontiers*

in Ecology and the Environment, vol. 15, issue 3, pp. 124-125, 2017.

[12] J. Wang, C. Liu, X. Fu, X. Luo, X. Li, "A three-phase approach to differentially private crucial patterns mining over data streams," *Computers & Security*, vol. 82, pp. 30-48, 2019.

[13] S. Hu, W. Bai, K. Chen, C. Tian, Y. Zhang, H. Wu, "Providing bandwidth guarantees, work conservation and low latency simultaneously in the cloud," *IEEE Transactions on Cloud Computing*, 2019, doi: 10.1109/TCC.2018.2890252.

[14] M. Du, Q. Wang, M. He, J. Weng, "Privacy-preserving indexing and query processing for secure dynamic cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 13, issue 9, pp. 2320-2332, 2018.

[15] Z. Zhang, P. Cheng, J. Wu, & J. Chen, "Secure State Estimation Using Hybrid Homomorphic Encryption Scheme," *IEEE Transactions on Control Systems Technology*, 2020.

[16] G. Bello-Orgaz, J. J. Jung, D. Camacho, "Social big data: Recent achievements and new challenges," *Information Fusion*, vol. 28, pp. 45-59, 2016.

[17] V. C. Storey, I. Y. Song, "Big data technologies and management: What conceptual modeling can do," *Data & Knowledge Engineering*, vol. 108, pp. 50-67, 2017.

[18] X. Jin, B. W. Wah, X. Cheng, Y. Wang, "Significance and challenges of big data research," *Big Data Research*, vol. 2, issue 2, pp. 59-64, 2015.

[19] E. Azhir, N. J. Navimipour, M. Hosseinzadeh, A. Sharifi, & A. Darwesh, "Query optimization mechanisms in the cloud environments: A systematic study," *International Journal of Communication Systems*, vol. 32, issue 8, pp. 3940, 2019.

[20] R. Sahal, J. G. Breslin, & M. I. Ali, "Big data and stream processing platforms for Industry 4.0 requirements mapping for a predictive maintenance use case," *Journal of Manufacturing Systems*, vol. 54, pp. 138-151, 2020.

[21] K. Hu, & G. Zeng, "Placing big graph into cloud for parallel processing with a two-phase community-aware approach," *Future Generation Computer Systems*, vol. 101, pp. 1187-1200, 2019.

[22] G. Iordache, "An Analysis of Service Level Agreement Parameters and Scheduling in Multi-Tenant Cloud Systems," in *Proceedings of the 22nd IEEE International Conference on Control Systems and Computer Science (CSCS)*, Bucharest, Romania, May 28-30, 2019, pp. 140-145.

[23] N. Wang, M. Matthaiou, D. S. Nikolopoulos, & B. Varghese, "DYVERSE: DYnamic VERtical Scaling in multi-tenant Edge environments," *Future Generation Computer Systems*, vol. 108, pp. 598-612, 2020.

[24] Y. Lu, & X. Zheng, "6G: A survey on technologies, scenarios, challenges, and the related issues," *Journal of Industrial Information Integration*, vol. 19, pp. 100158, 2020.

[25] S. Farooq, & P. Chawla, "A novel approach of asymmetric key generation in symmetric AES via ECDH," *International Journal of System Assurance Engineering and Management*, vol. 11, issue 5, pp. 962-971, 2020.

[26] L. Zhou, J. Chen, Y. Zhang, C. Su, & M. A. James, "Security analysis and new models on the intelligent symmetric key encryption," *Computers & Security*, vol. 80, 14-24, 2019.

***Jayapandian N**, He is working as an assistant professor at the Christ University, Department of Computer Science and Engineering, Bangalore, India. He completed Ph.D in the area of Data Security. His research interest includes information security, cloud computing, and grid computing. Dr. Jayapandian holds a Bachelor of Technology degree in Information Technology from IRTT, Anna University and Master degree in Computer Science and Engineering from KEC, Anna University. He published various research articles in reputed international journals. He published two book chapters in reputed publisher. He is an active reviewer of reputed international journals. He has participated in numerous national and international conferences and has made a remarkable contribution to cloud data security field and publishing several articles.*