Integration of Cloud Computing and Big Data: Security Challenges and Novel Security Algorithm

Khushi Ram, Prof (Dr.) Mukesh Singla

Department of Computer Science and Applications
Baba Mastnath University Rohtak

Abstract: Cloud Computing and Big Data are two transformative technologies that have revolutionized the way data is stored, processed, and managed. This work presents a survey of Cloud Computing and Big Data, focusing on the security and management challenges associated with both technologies. The study aims to explore the integration of these technologies and uncover new perspectives and opportunities for their combined use. The research investigates how Cloud Computing enhances the functionality of Big Data, addressing a gap in the scientific understanding of their integration. Additionally, the paper discusses the security challenges associated with integrating Big Data and Cloud Computing and proposes a novel security algorithm. The experimental results demonstrate the use of encryption algorithms such as AES, RC5, and RSA, along with the present model, to provide advanced privacy and security services. The findings highlight the potential of this integrated approach to deliver a scalable and secure service platform for managing and processing large volumes of data.

Keywords: Cloud Computing, Big Data, integration, management challenges, security challenges, privacy, encryption algorithms, scalability

I. INTRODUCTION

Cloud computing might function as a "base technology" for other technologies because of the distinctive services it offers. The ability to access and manage information, apps, and data from any location at any time is provided through a new generation of services. However, there is a certain kind of service that can involve a lot of data, and it is known as "Big Data" to refer to the surprisingly quick rise in data volume. In running their businesses, both of them encountered numerous difficulties. In the beginning of this work, we provide an overview of Big Data and Cloud Computing with a focus on their respective management and security challenges. The convergence of cloud computing and big data has transformed the landscape of modern computing. Cloud computing enables on-demand access to a shared pool of computing resources, while big data analytics allows organizations to extract valuable insights from large and complex datasets. This integration has fueled innovation across various industries, ranging from healthcare and finance to retail and manufacturing. However, this paradigm shift has raised concerns about the security of data stored and processed in cloud-based big data environments.

Security challenges in this integrated environment stem from the unique characteristics of both cloud computing and big data. Cloud computing introduces shared infrastructure, multi-tenancy, and remote data storage, which can potentially expose sensitive data to unauthorized access or data breaches. Big data, on the other hand, involves large-scale data processing, distributed storage, and the use of heterogeneous data sources, making it susceptible to data leakage, unauthorized data modification, and privacy breaches.The primary security challenges associated with the integration of cloud computing and big data include:

Data confidentiality and privacy: With sensitive data being stored and processed in the cloud, ensuring its confidentiality and privacy becomes crucial. Unauthorized access to data can lead to financial losses, reputational damage, and regulatory non-compliance. Additionally, privacy concerns arise when organizations share data across different domains for collaborative analysis or data monetization purposes.

Data integrity and trustworthiness: Maintaining the integrity of data is essential to ensure its accuracy and reliability. In a cloud-based big data environment, data integrity risks can arise from various sources, including data corruption during transmission, unauthorized modifications, and malicious activities. Trustworthiness of data sources and the integrity of analysis results also become critical factors.

Access control and identity management: With multiple users and organizations accessing and sharing data in the cloud, implementing robust access control mechanisms and efficient identity management becomes vital. Unauthorized access or weak authentication mechanisms can lead to data breaches, unauthorized data retrieval, or insider threats.

Data availability and resilience: In a cloud environment, ensuring continuous availability of data and services is crucial for business operations. However, the integration of big data and cloud computing may introduce challenges related to data availability, such as network latency, service disruptions, and system failures. These challenges can impact critical business processes and decision-making.

To address these security challenges, this research paper proposes a novel security algorithm specifically designed for the integrated cloud computing and big data environment. The algorithm aims to enhance data confidentiality, integrity, access control, and availability while considering the unique characteristics and requirements of both cloud computing and big data.

II. RELATED WORK

In attempt to combine Cloud Computing with Big Data, numerous research projects have been presented in recent years. The integration of Cloud Computing technology with Big Data technology has thus been the subject of prior literature research studies that we have investigated and analysed for the purposes of this study [1] [47-66]. The works are all listed below in order from oldest to newest.

To start out with, Takabi et al.'s [2] work explores challenges and improvements with the goal of offering a reliable cloud computing environment.Agrawal et al. [3] propose a kind of tutorial work that presents an organised view of the issues that application developers and DBMS (Database Management Systems) designers encountered in creating and implementing internet-scale applications.Ji et al. [4] present a number of Big Data processing techniques from system and application perspectives. Ji et al. address the main concerns of big data processing, including the Cloud Computing platform, Cloud architecture, Cloud database, and data storage scheme. This is specifically in connection with the view of Cloud data management and big data processing methods. Talia et al.'s [5] work aims to advance the Cloud from a computation and data management infrastructure to a pervasive and scalable data analytics platform, which calls for smart and scalable analytics services, programming tools, and applications.

Demirkan and Delen's [6] study proposes a conceptual framework for DSS in the cloud and discusses future research paths while taking into account a set of established needs for service-oriented DSS.

To continue, Fernandez et al. [7] concentrate on systems for large-scale analytics based on the MapReduce scheme and Hadoop, and they identify a number of libraries and software projects that have been built to help practitioners in order to handle a new programming model.

According to Khurana [8] in a different paper, depending on the workloads and access patterns that they support, BD systems might adopt several deployment paradigms. As a result, BD systems will be able to take advantage of public Cloud environments more efficiently if there are prospects for closer interaction between CC and BD.

Additionally, Castelino et al. [9] make an effort to emphasise the integration of BD with CC, which can act as a driving force for the business and IT sectors as well as data analytics in general.

Bohlouli et al [10] present a framework that facilitates accessible, efficient and always available knowledge bases for collaborative systems and reduces redundancy and costs by sharing the knowledge between individuals and experts.

Bohlouli et al [11] present a framework that provides an accessible, efficient and always available knowledge base for collaborative systems. The framework is designed to reduce the complexity of knowledge management and to create a platform for sharing information among different users in an organization. With this framework, users can access the same data from multiple sources, allowing them to quickly find the right information they need. Additionally, it enables the integration of new technologies into existing systems, making it easier for organizations to keep up with ever-evolving trends in their respective industries.

In their work, Inukollu et al [12] discuss the security issues related to Cloud Computing (CC), Big Data (BD), Map Reduce, and Hadoop environment. They focus on the main security threats that can arise in such environments, such as data leakage, malicious activities, and unauthorized access. They also present solutions that can be implemented to protect the systems from these threats. The solutions discussed include encryption techniques, authentication methods, and access control mechanisms. Finally, they provide a detailed analysis of the existing security measures and their effectiveness in protecting the systems from various attacks.

Ye et al.'s [13] proposal for a smart grid information and communication technology (ICT) framework is driven by big data and is cloud-based. The suggested ICT system provides utility companies with energy forecasts and customers with price forecasts. The present technique offers anonymity and nonrepudiation since it combines the functionalities of digital signature and encryption.

In their article, Assuncao et al. [14] present methods and parameters for BD analytics on cloud platforms. It focuses on four major Big Data and analytics topics. Assuncao et al. also point out potential shortcomings and suggest future research topics on Cloud-supported BD computing and analytics solutions.

Hashem et al. [15] evaluate the development of BD in CC and go over how BD storage solutions and Hadoop work together.

In their survey of BD and CC, Yang et al [16] discuss the benefits and drawbacks of applying CC to the problem of BD in the fields of the digital earth and pertinent science.

A strategy is put up by Dasoriya [17] to improve the efficacy, accuracy, and value of BD Analytics. The author is aware that it is possible to combine the use of several tools to create a system that is more effective.

Stergiou and Psannis [18] analyse BD and CC and their primary aspects, emphasising the security and privacy concerns of both technologies, and attempting to merge the functionality of BD and CC, with the purpose of examining the common features and discovering the benefits linked to security difficulties.

Simmhan et al.'s [19] main concern is a scalable software framework for the Smart Grid cyber-physical system. Additionally, this platform provides scalable machine-learning models for adaptive demand forecasting that have been verified on the campus micro-grid of the University of Southern California, as well as a portal for visualising consumption patterns.

III. CLOUD COMPUTING

Cloud Computing refers to the delivery of computing resources, including servers, storage, databases, networking, software, and analytics, over the internet. Rather than relying on a local server or personal computer, users can access and utilize these resources remotely through a network of servers hosted on the internet. As is already known, cloud computing has the potential to provide users with a number of useful capabilities, including computation, storage, services, and applications over the Internet [66]. The ability of the Cloud to be extended is limited by the fact that the sharing levels will vary for different delivery models, which in turn affects security and privacy. In particular, because of the special function of the Cloud's environment, the Cloud providers and the customers are eager to share the responsibility for security and privacy in Cloud Computing environments.

The cloud computing delivery data models are described in more depth below[20]:

SaaS: Offers often enable services by offering a significant number of integrated features, which may limit the extent to which clients can extend the services [20].

PaaS: aims to make it possible for developers to create their own apps on top of the platforms offered [20].

IaaS: This model can be developed the greatest. In this framework, the cloud service providers are required to offer some fundamental, low-level data protection capabilities [20].

A. Features

The Cloud Computing technology has some key characteristics that, like all technologies, define its functionality and "character." The following analysis and outline covers the key aspects of cloud computing.

Storage over Internet

Storage over the Internet is a technological framework that links servers and storage devices using Transmission Control Protocol/Internet Protocol (TCP/IP) networks and simplifies the deployment of storage solutions. Storage over Internet Protocol (SoIP) is another name for the Storage over Internet functionality. The SoIP might provide the customer with scalable and high-performance IP storage options. [21] [22] [23].

Service over Internet

This feature's primary goal is to be committed to users in order to assist users who want to leverage the Internet's effectiveness, speed, and ubiquity to turn dreams into accomplishments. [21] [22] [23].

Applications over Internet

According to the literature, the characteristic known as "Applications over Internet" refers to computer programmes that are created to replace human labour and run on a server, such as a cloud server, through an internet connection.[21] [22] [23].

Energy Efficiency

Energy efficiency is an attribute that can be characterised as a method of controlling and limiting the growth in energy usage. [21] [22] [23].

Computationally Capable

Cloud computing could make it possible for computational clouds to use ubiquitous and computationally demanding mobile applications. As a result, a system is said to be computationally capable when it satisfies the criteria for providing the user with the desired outcomes by doing the appropriate calculations. [21] [22] [23].

B. Security

Security research in cloud computing is a new growing area within the wider fields of computer, network, and information security. Data, apps, and the associated infrastructure of cloud computing are all protected by a wide range of policies, methods, and controls called "cloud computing security." [21] [22] [23].

Moreover, the encryption algorithms mix up the data using "a key" that can only be accessed by certified users [38]. As a result, based on the literature and research done to far, "Symmetric key encryption" is the most significant encryption method. Only one key is needed to encrypt and decrypt data when using the "Symmetric key encryption" method, and the most popular algorithm is AES. [24] [25].

Th**e** most crucial symmetric key encryption methods for cloud computing can be classified into one of two categories.n the beginning, the NIST recommends the AES (Advanced Encryption Standard) encryption method as a replacement for the DES encryption algorithm. Additionally, it features a changeable key length of 128, 192, or 256 bits, with a 256-bit default model. Additionally, depending on the key size, AES encrypts data blocks of 128 bits in 10, 12, and 14 rounds. AES encryption may be used on many platforms and is quick and adaptable, especially in small devices like mobile phones [24] .

The RC5 algorithm is the second kind of symmetric key encryption method that is vital for cloud computing. Ronald Rivest created RC5 in 1994. The "Rivest Cypher" or, alternately, "Ron's Code" is denoted by the letters R and C. While the key length for RC5 can be 32, 64, or 128 bits, its typical size is MAX2040 bits with a block size of 32, 64, or 128. The initial recommended parameter selections were a 64-bit block size, a 128-bit key, and 12 rounds. One of RC5's objectives was to stimulate research into and evaluation of these operations as cryptographic primitives. A variety of modular enhancements and eXclusive OR, XORs are also included in RC5. We can describe its algorithmic structure as being similar to a Feistel network. Thus, a few lines of code can be used to specify both the encryption and decryption routines. Additionally, the key schedule, which is frequently more sophisticated than the other algorithms, uses the binary expansions of both e and the golden ratio as sources of "nothing up my sleeve numbers" to expand the key using a largely one-way function. In reality, we can see that the RC5 is essentially denoted as RC5-w/r/b, where w is the word size in bits, r is the number of rounds, and b is the number of 8-bit bytes in the key. Despite all of its advantages, we might state that this algorithm's poor pace represents a drawback[24].

Additionally, the RSA method is crucial in relation to the other category of encryption techniques, known as asymmetric key encryption. A system for internet encryption and authentication known as RSA uses an algorithm that was created in 1977 by three scientists, Ron Rivest, Adi Shamir, and Leonard Adleman. The most popular encryption technique is based on this algorithm. Regarding the application of RSA, it may be said that it is the sole algorithm utilised for the production of private and public keys as well as the encryption mechanism. RSA may be the quickest encryption technique as a result. [24] .

C. Privacy and Securities Challenges

The literature review has presently shown us that the cloud computing environments can be characterised as multi-domain environments. Because of the potential for these settings to regard each domain as having unique security, privacy, and trust requirements, different techniques, interfaces, and semantics may be used. As a result, we are aware that those Cloud domains may represent distinct enabled services or other application or infrastructure components. [20].

As a result, and in accordance with the review of the literature, we can say that the most significant challenges to overcome in the field of cloud computing are as follows:

- Authentication and Identity Management
- Access Control and Accounting
- Trust Management and Policy Integration
- Secure-Service Management
- Privacy and Data Protection
- Organizational Security Management

We understand that the primary focus of these issues is on the protection of the data management services in a cloud computing environment.

IV. CLOUD COMPUTING & BIG DATA INTEGRATION

A number of studies must be performed in order to develop the optimum integration model between cloud computing and big data. We might discuss the contributions of Cloud Computing features to Big Data by drawing on prior relevant studies and our own research.

Table 1: Contribution of Big Data in Cloud Computing

Cloud Computing Features Big Data Features (5 Vs)	Storage over internet	Service over internet	Application over internet	Energy efficiency	Computationally Capable
Volume	X		X	X	
Velocity		X	X	X	X
.Variety		X		X	
Veracity	X		X		X
Value	X	X	X	X	X

Table 5.3 shows the characteristics of cloud computing technology in terms of the convenience it offers. It also lists the five key characteristics of big data, or 5 VS. The major goal of Table 1 is to demonstrate which specific Cloud Computing technology aspects contribute more and are therefore more closely tied to Big Data technology features. As we can see from Table 1, "Value" is the aspect of Big Data that is most impacted by the attributes of Cloud Computing. As we have already noted, value is related to data that is made up of enormous data sets. Therefore, it should be evident that this is the most important aspect of Big Data that contributes to Cloud Computing technology. In terms of cloud computing, "Applications over the Internet" and "Energy Efficiency" are the features that have been most impacted. The usage of the data through the network is the basis for both of these features. Applications may be able to extract sizable data sets, and grouping data into sizable data sets can improve the utilisation of power resources, creating a setting that is more energy-efficient. As a broad conclusion, we can see that these two technologies complement each other more in terms of many of their aspects.

Table 2: Contribution of Cloud Computing Models in Big Data Sources

Big Data Sources	SaaS Software as a Service	PaaS Platform as a Service	IaaS Infrastructure as a Service
Earth Sciences	X	X	X
Internet of Things	X	X	X
Social Sciences	X		
Business	X		X
Industry		X	X

The three Cloud Computing technology types and the primary Big Data sources are listed in Table 2. We may connect the requirement for using various Cloud Computing bottle models to the various sources that export Big Data through 2. Table 2 shows that "Internet of Things" is the source of big data that the cloud computing models have contributed to the most. According to our research, the Internet of Things is a key source that big data relies on. Additionally, it is relatively similar to all forms of cloud computing technology because of its use, which is specifically connected to the internet. "SaaS" and "IaaS" models have made the most contributions to cloud computing. As a result, we may draw the conclusion that cloud computing can support big data by providing the necessary hardware and software resources.

Big Data and Cloud Computing integration gives us the chance to increase the usage, management, and transfer of the massive data sets that make up Big Data, which are offered in settings based on Cloud Computing. Using this interface, it is possible to leverage cloud storage to access applications and information that could be generated by big data. Access to all the data and applications required for all the data that can be categorised as Big Data is provided via cloud computing to mobile and wireless users.

V. SECURITY METHOD FOR BIG DATA ENCRYPTION IN CLOUD ENVIROMENT

The literature review attributed us to the conclusion that the most rapid and effective encryption methods are AES, RC5, and RSA. AES also thought about improving the security environment for cloud computing technology, relying on earlier research in this area. Additionally, users have the option to create a more secure Cloud environment thanks to the symmetric encryption method of RC5 and the asymmetric encryption method of RSA.

Table 3: Comparison of AES, RC5 and RSA Algorithms

Algorithms Characteristics	AES	RC5	RSA
Year Founded	1998	1994	1977
Key Length	128, 192, or 256 bits	32, 64, or 128 bits	1024 – 4096 bits
Rounds of Encryption	10, 12, or 14	12	1
Type of Key Cryptography	Symmetric Key Encryption	Symmetric Key Encryption	Asymmetric Key Encryption
Certification	AES winner, CRYPT, REC, NESSIE, NSA	AES finalist	PKCS#1, ANSI X9.31, IEEE 1362
Algorithm Speed	Very Fast	Very Fast	Very Fast

The three aforementioned encryption algorithms (AES, RC5, and RSA) that have been analysed and employed to get to at our experimental suggestion are listed in Table3 along with their main properties. Their speed is one of their essential characteristics that is significant in our study, as we have already indicated. Due to their rapid response during the encryption process, all three techniques can be considered fast algorithms. As a result, one important area in which they greatly diverge is the number of rounds required for encryption; although RSA just requires one round, AES requires 10, 12, or 14 rounds, and RC5 requires 12.

In order to offer the best encryption environment for Big Data in Cloud Computing applications our suggested technique gathers and combines all the advantages of the three algorithms. Therefore, by providing a highly innovative and scalable efficient service platform, we may accelerate the advancements of Cloud Computing and Big Data technologies using our present model. The following algorithm can be suggested and introduced as a consequence for a more secure use of Big Data in Cloud Computing.

VI. COMPARATIVE ANALYSIS

The authors K. Gai et al. [26] focus on the privacy issue and provide a novel data encryption strategy dubbed Dynamic Data Encryption Strategy (D2ES), which focuses on selective data encryption and applies privacy classification techniques under time limitations. They conclude by presenting tests that assess the effectiveness of the suggested D2ES and demonstrate the privacy benefit.

H. Matallah et al. [27] suggest a method for improving the Hadoop service metadata to maintain consistency without significantly compromising performance and scalability of metadata by suggesting a mixed solution between centralization and distribution of metadata for improving the performance and scalability of the model.

S. K. Mishra et al. [28] analysed how much energy is used when using a variety of cloud computing services, and they succeeded in implementing policies that support green cloud computing. Additionally, in order to shorten the life of the cloud system and use less energy, the scientists presented an adaptive job allocation algorithm for the heterogeneous cloud environment. The suggested evaluation scenarios were also tested in the CloudSim simulation environment.

In terms of the optimised network resource usage, such as network bandwidth and data storage units, R. Chaudhary et al.'s [29] unique SDN-based Big Data management scenario is presented. Furthermore, they think that by implementing their suggested fix, the programmers would be able to deploy and examine real-time traffic patterns for upcoming Big Data apps in MCE.

Y. Wen et al. [30] model the challenge of how to schedule workflow with such data privacy protection constraints, while minimising both execution time and financial cost for Big Data applications on Cloud environment as a multi-objective optimisation problem and propose a Multi-Objective Privacy-Aware workflow scheduling algorithm, named MOPA. Customers of the cloud may be provided with a range of Pareto tradeoff solutions using the present technique.

Table 4: Contribution of Big Data in Cloud Computing

Big Data & Cloud Computing Integration Challenges	Privacy	Security	Energy Eff	Access Control	Computation (Processing) & Analysis	Managemen
Gai et al. [26]	X	X				
Matallah et al. [27]					X	X
Mishra et al. [28]			X		X	
Ghaudhary et al. [29]				X	X	X
Wen et al. [30]	X	X				
Present method	X	X		X	X	X

The majority of the attributed works, as shown in Table 4, focus on and attempt to address problems with computation (processing) and analysis. Additionally, the majority of the former relative's jobs relate to management, security, and privacy. Energy Efficiency and Access Control are the issues that are not at the forefront of research focus. Consequently, we may draw the conclusion that there are numerous unresolved problems in the area of Cloud Computing and Big Data integration. As a conclusion, we recognise the need for additional research in the area of Big Data Security and Management in the Cloud Computing environment, and as a result, we propose a new data encryption method in the Cloud environment that aims to address and improve issues like Big Data Security and Management.

VII. EXPERIMENTAL ANALYSIS RESULT

A. Comparative Result

Considering the advantages of Big Data and Cloud Computing's security models and algorithms, we might be able to exploit the integration model to our advantage. The new integration model will handle all types of block sizes and key sizes that are typically used for Big Data in a cloud computing environment, and it also has a strong chance of gaining from instruction-level parallelism.The use of cloud-based services and applications to connect devices and sensors, generate large amounts of data, and enable them to share their data through the cloud while lowering security risks are just a few of the useful operations that could be accomplished through this integration.However, there are still a lot of other advantages and drawbacks that need to be dealt with through the integration of cloud computing with big data, including the management and security issues, as well as the overall use of both technologies.The three tables above (Table 5, Table 6, and Table 7) emphasise the salient features of the three encryption algorithms that were previously discussed and used in an effort to integrate Big Data and Cloud Computing with regard to security challenges. They also touch upon some of the management of data challenges. Table 5 outlines the key aspects of the AES encryption method that both Cloud Computing and Big Data contribute to, as well as how much of a contribution each makes to the integration model. Table 6 also shows which key aspects of the RC5 encryption technique are also contributed by Cloud Computing and Big Data, as well as how fully its integration model is contributed. Finally, Table 7 shows which key aspects of the RSA encryption method also contribute to Cloud Computing and Big Data, as well as how fully its integration model does so.

Table 5: AES Contribution in Cloud Computing and Big Data.

AES Characteristics	Key length	Rounds	Certifications	Speed
Cloud Computing	X	X	X	
Big Data	X		X	X
Integration model	X	X	X	X

Table 6: RC5 Contribution in Cloud Computing and Big Data.

RC5 Characteristics	Key length	Rounds	Certifications	Speed
Cloud Computing	X	X	X	
Big Data	X			X
Integration model	X	X	X	X

Table 7: RSA Contribution in Cloud Computing and Big Data.

RSA Characteristics	Key length	Rounds	Certifications	Speed
Cloud Computing	X	X	X	
Big Data			X	X
Integration model	X	X	X	X

B. Experimental Result

Numerous simulations have been conducted in order to demonstrate how well our present model works. We compared the functionality of our suggested model over time with the functions of the AES, RC5, and RSA existing algorithms using the experimental situations we created. These simulations and their outcomes provide us the chance to see that a lot of work has gone into providing a more secure and effective model. Figure 1 depicts four experimental situations that take into account how well the four algorithms (AES, RC5, RSA, and the present model) perform when processing data in a given amount of time. Through these examples, we can see that applying our suggested paradigm will result in better data processing than the AES, RC5, and RSA encryption techniques that are currently in use. Additionally, the following explanations are provided for figures 1: line red denotes AES, line green denotes RC5, line yellow denotes RSA, and line blue denotes our suggested model. Figures 2, Figure 3, Figure 4 show the AES, RC5 and RSA encrypted individual Performance of data processed result. Figure 5 show the comparison results of AES, RC5 and RSA algorithm of data processed. Figure 6 show the all four algorithm combined result. Figures 6: line red denotes AES, line green denotes RC5, line yellow denotes RSA, and line blue denotes our suggested model. Thus, as we can see from figure 6 we could analyse more data simultaneously with our suggested approach.

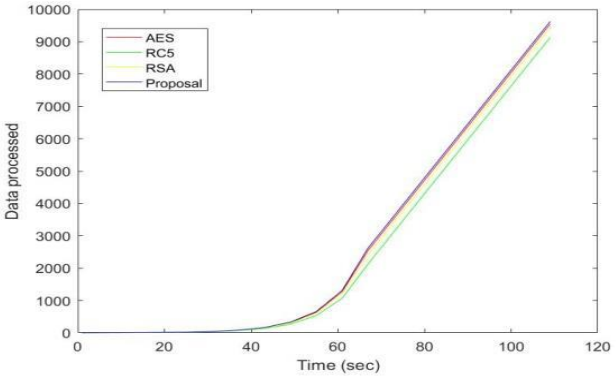

Figure 1: Performance of data processed comparison of the AES, RC5, RSA & Present model.

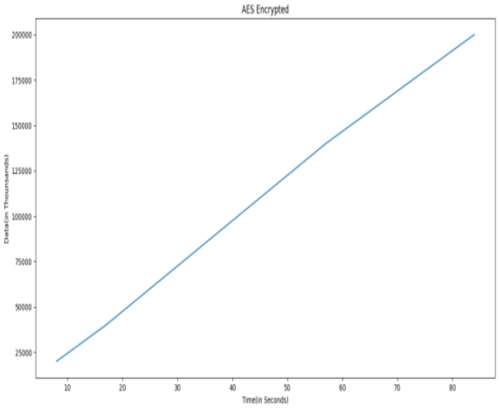

Figure 2: Performance of data processed of the AES

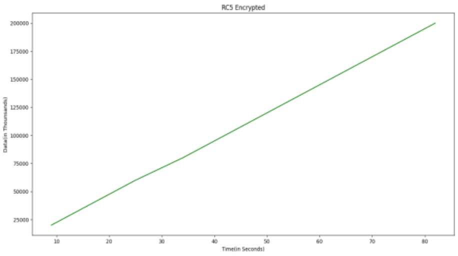

Figure 3: Performance of data processed of the RC5

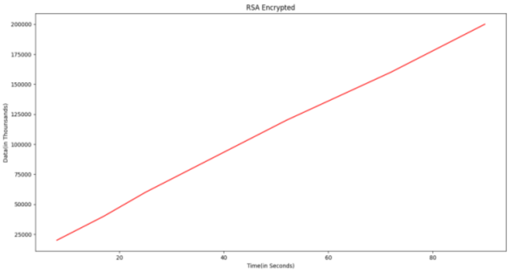

Figure 4: Performance of data processed of the RSA

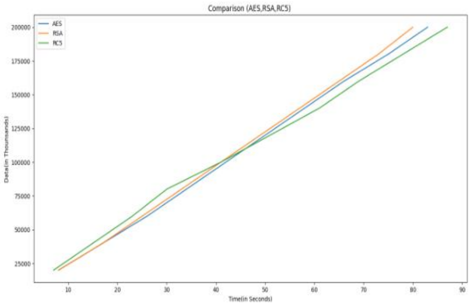

Figure 5: Performance of data processed comparison of the AES, RC5, RSA

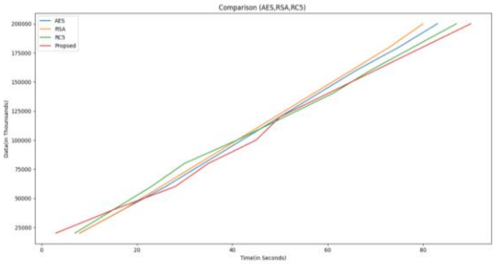

Figure 6: Performance of data processed comparison of the AES, RC5, RSA & Present model

VIII. CONCLUSION

It is widely accepted that even though cloud computing provides a lot of potential, it also has a lot of restrictions. As a result, we examined the security and management issues associated with Big Data and Cloud Computing in this work.In particular, we have merged them to demonstrate the shared traits and to determine the advantages of their integration. In order to close the existing scientific gap in this area, we presented the Big Data contribution to Cloud Computing. Additionally, the present study demonstrated how Cloud Computing enhances Big Data's functionality.Finally, we reviewed the security concerns surrounding the combination of big data and cloud computing and presented an improved security architecture. The present model extends the advancements of Cloud Computing and Big Data, and experimental results that are also shown at the conclusion of this study use the encryption techniques AES, RC5, and RSA. Finally, the provided algorithm model was used to study the security issues associated with the integration of Cloud Computing and Big Data. In addition, it demonstrated how the three encryption algorithms examined in this work contribute to the integration model of Cloud Computing and Big Data. As a result, based on this, we could decide to focus future research on the fusion of cloud computing and big data. In order to have a successful integration model, it is necessary to clarify or reduce the security and management issues associated with the data that is transmitted and stored in the Cloud.

REFERENCES

[1] C. Stergiou, K. E. Psannis, “Efficient and secure BIG data delivery in Cloud Computing”, Springer, Multimedia Tools and Applications, vol. 76, issue: 21, pp. 22803–22822, November 2017.

[2] H. Takabi, J. B. D. Joshi, G.-J. Ahn, “Security and Privacy Challenges in Cloud Computing Environments”, IEEE Security & Privacy, vol. 8, issue: 6, pp. 24-31, December 2010. [DOI: 10.1109/MSP.2010.186]

[3] D. Agrawal, S. Das, A. El Abbadi, “Big data and cloud computing: current state and future opportunities”, ACM, in Proceedings of the 14th International Conference on Extending Database Technology, EDBT/ICDT ’11, pp. 530-533, 21-24 March 2011, Uppsala, Sweden.

[4] C. Ji, Y. Li, W. Qiu, U. Awada, K. Li, “Big Data Processing in Cloud Computing Environments”, in Proceedings of IEEE 12th International Symposium on Pervasive Systems, Algorithms and Networks, 13-15 December 2012, San Marcos, TX, USA.

[5] D. Talia, “Clouds for Scalable Big Data Analytics”, IEEE Computer, vol. 46, issue: 5, pp. 98-101, May 2013 [DOI: 10.1109/MC.2013.162]

[6] H. Demirkan, D. Delen, “Leveraging the capabilities of service-oriented decision support systems: Putting analytics and big data in cloud”, Elsevier, Decision Support Systems, vol. 55, issue: 1, pp. 412-421, April 2013. [DOI: 10.1016/j.dss.2012.05.048]

[7] A. Fernandez, S. del Rio, V. Lopez, A. Bawakid, M. J. del Jesus, J. M. Benitez, F. Herrera, “Big Data with Cloud Computing: an insight on the computing environment, MapReduce, and programming frameworks”, Wiley Online Library, Wires Data Mining and Knowledge Discovery, vol. 4, issue: 5, pp. 380-409, September 2014.

[8] A. Khurana, “Bringing Big Data Systems to the Cloud”, IEEE Cloud Computing, vol. 1, issue: 3, pp. 72-75, September 2014. [DOI: 10.1109/MCC.2014.47]

[9] C. Castelino, D. Grandhi, H. G. Narula, N. H. Chokshi, “Integration of Big Data and Cloud Computing”, International Journal of Engineering Trends and Technology (IJETT), vol. 16, no. 2, pp. 100-102, October 2014.

[10] M. Bohlouli, F. Merges, M. Fathi, “Knowledge integration of distributed enterprises using cloud based big data analytics”, in Proceedings of IEEE International Conference on Electro/Information Technology, 5-7 June 2014, Milwaukee, WI, USA.

[11] V. N. Inukollu, S. Arsi, S. R. Ravuri, “Security Issues Associated with Big Data in Cloud Computing”, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.3, pp. 45-56, May 2014.

[12] F. Ye, Y. Qian, R. Q. Hu, “An Identity-Based Security Scheme for a Big Data Driven Cloud Computing Framework in Smart Grid”, in Proceedings of IEEE Global Communications Conference (GLOBECOM 2015), 6-10 December 2015, San Diego, CA, USA.

[13] M. D. Assuncao, R. N. Calheiros, S. Bianchi, M. A. S. Netto, R. Buyya, “Big Data computing and clouds: Trends and future directions”, Elsevier, Journal of Parallel and Distributed Computing, volumes 79-80, pp. 3-15, May 2015.

[14] I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, S. U. Khan, “The rise of “big data” on cloud computing: Review and open research issues”, Elsevier, Information Systems, vol. 47, pp. 98-115, January 2015.

[15] C. Yang, Q. Huang, Z. Li, K. Liu, F. Hu, “Big Data and cloud computing: innovation opportunities and challenges”, International Journal of Digital Earth, vol. 10, issue: 1, pp. 13-53, 2017. [DOI: 10.1080/17538947.2016.1239771]

[16] R. Dasoriya, “A review of big data analytics over cloud”, in Proceedings of IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia 2017), 5-7 October 2017, Bangalore, India.

[17] C. Stergiou, K. E. Psannis, “Algorithms for Big Data in Advanced Communication Systems and Cloud Computing”, in Proceedings of IEEE 19th Conference on Business Informatics (CBI 2017), 24-27 July 2017, Thessaloniki, Greece.

[18] F. Kelbert, F. Gregor, R. Pires, S. Kopsell, M. Pasin, A. Havet, V. Schiavoni, P. Felber, C. Fetzer, P. Pietzuch, “SecureCloud: Secure big data processing in untrusted clouds”, in Proceedings of Design, Automation & Test in Europe Conference & Exhibition (DATE 2017), 27-31 March 2017, Lausanne, Switzerland.

[19] Y. Simmhan, S. Aman, A. Kumbhare, R. Liu, S. Stevens, Q. Zhou, V. Prasanna, “Cloud-Based Software Platform for Big Data Analytics in Smart Grids”, IEEE Journal of Computing in Science & Engineering, vol. 15, issue: 4, pp. 38-47, August 2013.

[20] C. Stergiou, K. E. Psannis, “Efficient and secure BIG data delivery in Cloud Computing”, Springer, Multimedia Tools and Applications, vol. 76, issue: 21, pp. 22803–22822, November 2017.

[21] G. Md Whaiduzzaman et al, “A Study on Strategic Provision of Cloud Computing Services”, The Scientific World Journal, pp. 1-8, June 2014.

[22] S. K. Garg, S. Versteeg, R. Buyya, “A framework for ranking of cloud computing services”, Future Generation Computer Systems, vol. 29, issue: 4, pp.012–1023, 2013.

[23] C. Stergiou, K. E. Psannis, B.-G. Kim, B. Gupta, “Secure integration of IoT and Cloud Computing”, Elsevier, Future Generation Computer Systems, vol. 78, part 3, pp. 964-975, January 2018. [DOI: 10.1016/j.future.2016.11.031].

[24] Randeep Kaur, Supiya Kinger, "Analysis of Security Algorithms in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 3, no. 3, pp. 171-176, March 2014.

[25] Yogesh Kumar, Rajiv Munjal, Harsh Sharma, “Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures”, IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, October 2011.

[26] C. Stergiou, A. P. Plageras, K. E. Psannis, B. B. Gupta, “Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network”, Springer, Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Multimedia Systems and Applications, 2019.

[27] K. Gai, M. Qiu, H. Zhao, “Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing”, IEEE Transactions on Big Data, pp. 1-1, in Press, May 2018. [DOI: 10.1109/TBDATA.2017.2705807]

[28] H. Matallah, G. Belalem, K. Bouamrane, “Towards a New Model of Storage and Access to Data in Big Data and Cloud Computing”, International Journal of Ambient Computing and Intelligence (IJACI), vol. 8, issue: 4, pp. 31-45, October-December 2017. [DOI: 10.4018/IJACI.2017100103]

[29] S. K. Mishra, D. Puthal, B. Sahoo, S. K. Jena, M. S. Obaidat, “An adaptive task allocation technique for green cloud computing”, Journal of Supercomputing, vol. 74, issue: 1, pp. 370-385, January 2018. [DOI: 10.1007/s11227-017-2133-4]

[30] R. Chaudhary, G. S. Aujla, N. Kumar, J. J. P. C. Rodrigues, “Optimized Big Data Management across Multi-Cloud Data Centers: Software-Defined-Network-Based Analysis”, IEEE Communications Magazine, vol. 56, issue: 2, pp. 118-126, February 2018. [DOI: 10.1109/MCOM.2018.1700211]