RESEARCH ARTICLE OPEN ACCESS

AN ENHANCED SECURITY MODEL ON CLASSIFED DATA IN CLOUD COMPUTING USING CRYPTOGRAPHY AND DIGITAL WATERMARKING

Alpha Baba Garba*, **, **SouleyBoukari****
*(Department of Computer Science, Kaduna State College of Education GidanWaya, Nigeria.
Email: babandolee@gmail.com)
** (Department of Mathematical Sciences
Abubakar Tafawa Balewa University
Bauchi, Nigeria.
Email: bsouley2001@yahoo.com)

----------**********----------

Abstract:
Cloud Computing provides different services to users on request basis through the use of the internet. One major concern of the cloud is the security risks of the data; this has posed serious issues in trusting the security and integrity of data when exposed to the cloud. This work proposed an enhanced security model on classified data using different cryptographic techniques using Advanced Encryption Standard (AES), Rivest Shamir Adleman (RSA) and digital watermarking to improve the security of data stored in the cloud. The proposed system was implemented and simulated using Java programming toolkits with Netbeans IDE and cloudsim simulator. The work piloted a performance analysis of the existing system using K-NN and Improved Naïve Bayes algorithms and proposed system using improved Naïve Bayes and Modified K-NN algorithms. The results of the simulated system show that Modified K-NN algorithm performed significantly better than Improved Naïve Bayes algorithm in respect to data classification time of 665.60ms and 600.00ms and accuracy of the classified data having 97% and 98.26% respectively. Encryption time comparison of different cryptographic techniquesfor both the existing and proposed system depicts that Improved Naïve Bayes algorithm has RSA algorithm as 147462.40ms and AES algorithm with 2782.20ms. The Modified K-NN algorithm has 145692.80ms for RSA algorithm while AES algorithm has 2656.40ms. On the other hand the decryption time comparison of Improved Naïve Bayes algorithm has RSA algorithm as 36918.00ms with AES algorithm having 1070.40ms. The Modified K-NN algorithm has 36528.00ms for RSA algorithm and AES algorithm has 965.40ms. This work recommends that the proposed methodology and other machine learning algorithms be adopted by cloud service providers to improve on the classified data stored in cloud considering their security needs and sensitivity level. This will increase the confidence of their client and guaranteeing secured security in terms of data transfer and security of data store in cloud devoid of any enticing attack or mutilation on the data from malicious users.

Keywords — ***Cloud computing, Data classification, Machine learning, Modified K-NN, Naïve Bayes, Cryptographic and Digital watermarking.***

----------**********----------

I. INTRODUCTION

The advent of information technology (IT) has attracted so many organizations into adopting and using the facilities for data transfer, storage and management [16]. The current hype in the use of information and communication technology such as cloud computing, mobile cloud computing etc. has reduced so much stress for organization and individuals in managing their data and facilitates access to the data at convenience [11]. The most fast growing technology in the world of information technology today is the cloud computing [5].Cloud computing is a framework that provides access to variety of services to be utilized by users on demand and payable at minimal cost [14]. The infrastructure of cloud computing curtails the stress of buying and managing resources by diving into the available resources on the cloud [14]. The paradigm shift in cloud computing is to make data and information ubiquitous for easy outsourcing and used on the cloud [22],[7].

With all the good benefits offered by cloud computing yet, it has been accompanied with serious drawback of security concern to users [30]. This is because data information deployed to the cloud are managed by third party. This has posed a serious issue in trusting the security and integrity of data when exposed to the cloud. In order to curtail the security fear that has gripped many cloud users and provide assurance for the safety of data stored in the cloud, some security techniques were

developed and used. Among the developed security techniques used to provide security to data in the cloud are cryptography, steganography and watermarking [23].

Cryptography is a technique used to make data unreadable to unauthorized users. It converts the plain data or information into a scramble format that cannot be understood by intruders termed as encryption. There are two different types of cryptography techniques such as the symmetric encryption technique and asymmetric encryption technique. The symmetric method uses the same key for encrypting and decrypting of user data. In contrast the asymmetric methods use two keys for the encryption and decryption termed as public and private key. The public key is known to all while the private key is only known to the intended user [19].

Likewise, digital watermarking technique is used to watermark a data in order to ascertain its integrity at the point of access by the intended users. This is done in order to detect changes or unauthorized attempt on the data [12].

The major challenge in applying these different developed techniques in order to secure data stored in the cloud is that they are used across all the data in respective of sensitive and non-sensitive data. This has caused a lot over head in processing and accessing secured data in the cloud [30].

In view of that, the needs to develop a technique that will be applied to categorized sensitive and non-sensitive data and provide security based on the level of sensitivity of the data in the cloud for easy access to the data is expedient and also provide temper roofing techniques in order to notice any attempt on the classified and protected data.

Therefore, this work proposes a security model that will protect secret data and revealed illegal attempt on secured data in the cloud using cryptography and digital watermarking.

II. REVIEW OF RELATED WORK

[11], in there study, A Secure Data Classification Model for Achieving Data Confidentiality and Integrity in Cloud Environment. The proposed a secure data classification model using novel boosting supervised machine learning approach to achieve data security in the cloud using data classification and hybrid encryption method.

According to [30], A Secure Cloud Computing Model based on data classification to secure data in the cloud and obtained a secured cloud computing model based on data classification through minimize overhead and data processing time using different security techniques and variable key sizes.

[27], in their work, Data Classification for achieving Security in cloud computing presented a secured data classification in the cloud based on Security level of data to improve security in cloud based on data classification using encryption technique.

[31], Protecting Data in Personal Cloud Storage with Security Classifications and provided Data security in the cloud based on categorization and enhanced data access and security using data classification and encryption.

In their work, [24], proposes Application of Intelligent Data Mining Approach in Securing the Cloud Computing through analyzing security strength in the cloud using Chaid Algorithm and analyzes the robustness of secured data classification in the cloud using simple decision tree model Chaid Algorithm.

[26], in their study purported aSurvey on Data Classification and Data Encryption Techniques Used in Cloud Computing. Surveyed the existing security techniques used in the cloud and data classification and came up with different encryption techniques used in providing secured data in the cloud.

[18], Secure Model for Cloud Computing using Data Classification Methodology, proposed a framework for data authentication in the cloud based on data sensitivity level that Provide a secured data classification in the cloud using encryption and authentication scheme.

[25], in their paper KNN File Classification for Securing Cloud Infrastructure proposed an innovative Classifier QoS. This automated data classification approach is an extension to smart QoS which uses RSA algorithm to provide encryption for strictly confidential file, symmetric encryption for confidential file and KNN algorithm for data classification.

On the other hand, [21], Enhancing Cloud Security with automatic Data Classification and appropriate Encryption Algorithms, to achieving a high security using automatic data classification in cloud computing and addressed Data classification and security using Naïve Bayes classifier algorithm, RSA algorithm and Unicode encodes technique.

[29], opined that, Secure Cloud Model using Classification and Cryptography could be achieved through data classification approached based on data confidentiality and secured data classification to achieve a secured model using AES, RSA, Elgamma and Hashing Algorithm in the cloud.

[20], in their study An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E - LSB Encoding technique Proposed a technique for enhancing the security of cloud data using cryptography, steganography, and hash function for a better security of the data using the Blowfish encryption algorithm for encrypting the secret message and for steganography, E-LSB based steganography is used.

[28], Classification of Data to Enhance Data Security in Cloud Computing Proposed a classification of data based on sensitivity rating (SR), analysis of existing security mechanism in cloud, application of suitable encryption technique as per the SR to achieved. Data Classification based on three essential parameters of security, confidentiality, integrity and availability, also known as CIA triad was achieved.

[10], in their work, HESSIS: Hybrid Encryption Scheme for Secure Image Sharing in a Cloud Environment, A hybrid algorithm, Hybrid Encryption Scheme for Secure Image Sharing (HESSIS) is proposed to secure data while sharing. Proposed scheme combined secure hashing algorithm-3, Elliptic Curve and Advanced encryption algorithm to enhance the security.

[4], Secured cloud computing for medical data based on watermarking and encryption which proposed a secured medical cloud for archiving and transmission of medical data (images and reports). This is possible through low complexity algorithm for medical image encryption using LSB watermarking method for hiding the patient information in the medical imaging.

[13], To Apply Watermarking Technique in Cloud Computing to enhance Cloud Data Security, Proposes a Digital Watermarking Technique to enhance the security and robustness of Cloud Data and Employed Watermarking Technology to provide secured & reliable data in the cloud using GLCM & PCA algorithms. The result obtained provided cloud security using watermarking technology of copyright protection for Cloud Computing.

[9], Image Security using Digital Image Watermarking and Visual Cryptography Techniques proposes a secure protection for digital image based on watermarking and visual cryptography and employed digital watermarking in the protection of digital information which uses various Visual Cryptography and Digital Image Watermarking techniques are explained in real time application.

[3], Data Security in Cloud Computing Using Cryptographic Algorithms: A Review which proposed a technique for enhancing the security of cloud using cryptographic algorithms. The results provided secured a data using different Cryptography techniques in the Cloud Eliminate data privacy using cryptography algorithms.

[6], A Survey: Data Security in Cloud using Cryptography and Steganography proposes a technique to Secured Cloud Data using Cryptography and Steganography and provided secured data security in cloud using cryptography and steganography to provide security of data in the cloud.

Considering the review of related literatures, the researchers provide solution to secured data classification on the cloud using encryption technique. Their work either addresses the problem using a single encryption technique or hybrid encryption technique. The challenge with the use of only encryption method to provide data protection as stated by [4], is that encryption techniques do not hide the existence of data communication or provide techniques to identify unauthorized attempts on secured data.

Therefore, the need to come up with a technique that will provide protection on data and also point out illegal attempt on protected data is eminent.

In view of that, this work proposed a security technique using cryptography and digital watermarking in order to protect secret data and illegal attempt of secured data in the cloud.

III. METHODOLOGY

This research work proposes an enhanced data security classification in cloud computing using cryptography and digital watermarking technique. The major concern of the work is to develop an enhanced security technique used on classified data in the cloud based on their confidentiality and integrity levels in order to achieve strong security, integrity and improved processing time on data. Cryptography is mostly used to secure the different types of data in the cloud. Meanwhile, Cryptography provides confidentiality protection on the data stored on the cloud without strong level of integrity on the data in the case of illegal access attempt. In this work we propose to combine cryptography and digital watermarking techniques to provide confidentiality and integrity on the classified data stored in the cloud in order to protect and detect illegal access attempt on the stored data. The proposed system works by first applying cryptography technique on the classified data. After which the digital watermarking method is applied on the sensitive data in order to detect illegal attempt on the data.

A. *PROPOSED SYSTEM*

This work proposed to improve on the existing system by proposing a secured data classification using the combination of cryptography and digital watermarking in order to provide strong integrity on the data uploaded to the cloud and to evaluate the performance of the proposed system against [].

We aim to develop an improved security technique on classified data used in the cloud to secure highly sensitive, sensitive and basic data. However we propose the use of AES encryption algorithm to protect non-sensitive (basic) data, RSA algorithm to encrypt sensitive data and the encrypted sensitive data is concealed using digital watermarking technique for highly sensitive data uploaded to the cloud for integrity check.

B. *COMPONENTS OF THE PROPOSED SYSTEM*

The major components that constitute the proposed system framework are:

1. **Virtual Cloud environment:** Cloud simulator, Cloudsim consists of library which provides simulation environment for the system to be simulated and experimented with on cloud and also described virtual machines, data centers users and applications.
2. **Data Classification:** In this proposed framework, we proposed a secure data classification technique using machine learning Modified K-NN algorithm which classified data according to level of its sensitivity.
3. **Non Sensitive (Basic):** These are data that are categorized as non-critical to individuals or organizations used by the public via internet such as marketing materials, press announcements etc. These data are securely uploaded on cloud by encrypting them with AES algorithm.
4. **Sensitive:** These are data types that are categorized as being of medium sensitivity degree which cannot be access by any unauthorized person in the cloud which are for non-public view such as personal files, corporate data, medical/health data, specific intellectual property and most data that are access frequently or on daily basis. These sensitive data are securely uploaded on cloud by encrypting the data using RSA algorithm.
5. **Highly Sensitive:** These are critical and very important data of individuals or organizations which if lost or destroyed would have a severe impact on an individual or organization which among others include; Personal data (like social security number, national identification number, biometric verification number), financial records, and government data others include; legal data, authentication data and military data which are securely uploaded on cloud by watermarking the encrypted sensitive data using digital watermarking technique in other to notice any attempt or change on the data by unauthorized persons or entity.

C. *ARCHITECTURE OF THE PROPOSED SYSTEM*

The conceptual framework of the proposed system is shown as in Figure 1.

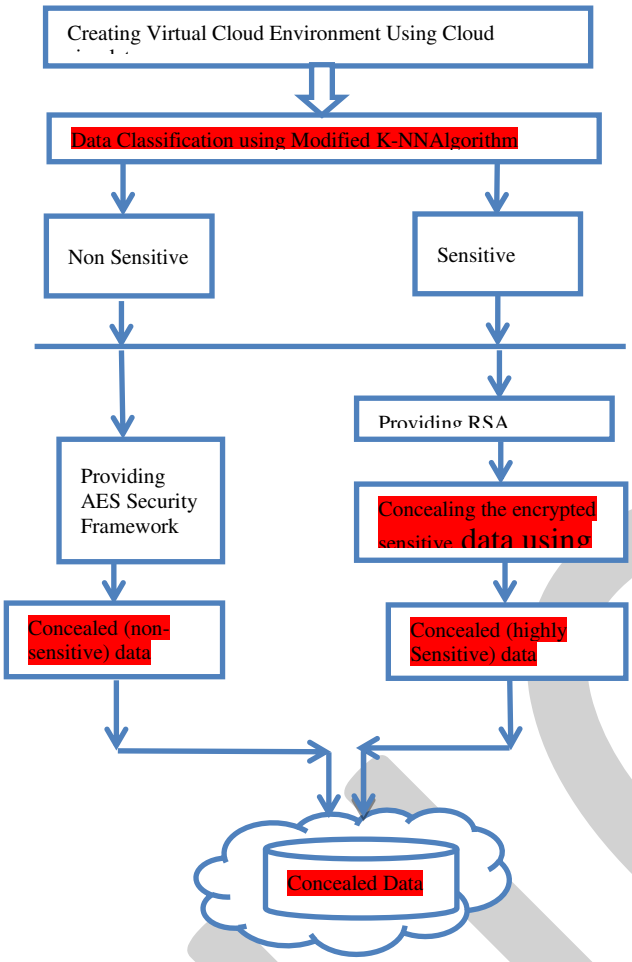

Figure 1: Architecture of the proposed system

D. *WORKING PRINCIPLE OF THE PROPOSED SYSTEM*

In this work, we propose to develop and enhanced security technique on classified data to provide strong security and check integrity on the data stored in the cloud. This is to facilitate access to the stored data in the cloud and processing time of sensitive and non-sensitive data. The working procedure of the proposed system is described as follows:

Step 1: Start

Step 2: Create Data

Step 3: Classify data into Non Sensitive and Sensitive using Modified K-NN algorithm.

Step 4: IF data is non sensitive THEN

Step 5: Encrypt data using AES encryption algorithm

Step 6: IF data is sensitive THEN

Step 7: Encrypt data using RSA encryption algorithm

Step8: Conceal the encrypted sensitive data using watermarking technique to obtained highly sensitive data

Step 9: Stop

IV. RESULT AND DISCUSSION

This section discusses the results of the simulated system. The experiments maintained the same data sets (train data and test data) for both the existing system (which compared K-NN with Improved Naïve Bayes algorithms) and the proposed system (which compared Improved Naïve Bayes algorithm with the Modified K-NN algorithm) to analyze the performance of the different algorithms.

RESULTS

The results for the experiment and simulation of the existing and proposed systems are described in this section. To evaluate the performance of the proposed security model, the experiment was re-run five times (test samples) for both the existing and the proposed methodology, the results obtained described the best performance system.

Test Case 1: Classification Time Comparison

Table 1 below shows the results of five different simulated test case samples for the existing and the proposed systems. The Average classification time of the different algorithms is used for the comparative analysis.

Table 1: CLASSIFICATION TIME COMPARISON

Test Sample	KNN	Improved Naive Bayes	Modified KNN
Run 1	903	672	609
Run 2	903	672	594
Run 3	887	672	594
Run 4	881	641	609
Run 5	878	671	594
Total	**4452**	**3328**	**3000**
Average Classification time	**890.40**	**665.60**	**600.00**

Figure 2a below show a graphical representation of results obtained from five different run simulation tests of both the existing and the proposed system.

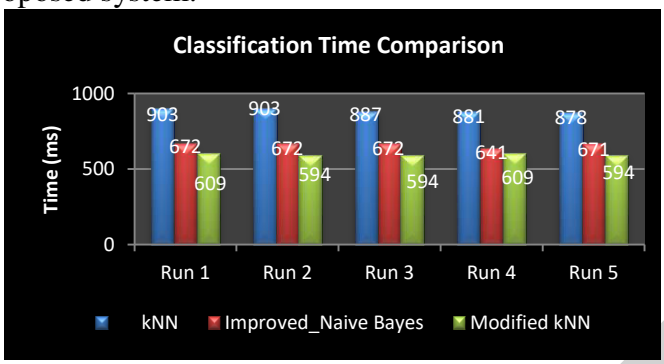

Figure 2a: Performance analysis of classification time based on five different run cases.

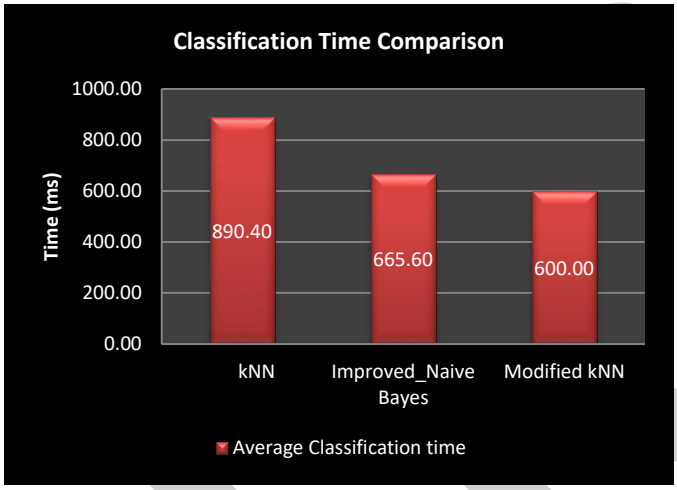

Figure 2b: Performance analysis on the basis of classification time

Figure 2 above, shows the graphical representation of the different algorithms performance analysis on the basis of classification time comparison. K-NN algorithm has 890.40ms, Improved Naïve Bayes algorithm is having 665.60ms and Modified K-NN algorithm having 600.00ms. The lowest value signifies the best algorithm classification time. The proposed Modified K-NN algorithm has shown to have performed better than the existing improved naïve Bayes algorithm.

Test Case 2: Accuracy Comparison

Table 3 below illustrates different re-run experiment (test sample) for the existing and the proposed systems. The Average Accuracy of the classified data is obtained and used for comparative analysis.

Table 2: Accuracy Comparison

Test Sample	KNN Algorithm	Improved Naive Bayes Algorithm	Modified KNN Algorithm
Run 1	71.60	97.0	98.3
Run 2	71.60	97.0	98.3
Run 3	71.60	97.0	98.3
Run 4	71.60	97.0	98.3
Run 5	71.60	97.0	98.3
Total	**358.02**	**485.00**	**491.29**
Average Accuracy	**71.60**	**97.00**	**98.26**

Figure 3a below show a graph illustration of results obtained from five different run simulation tests of both the existing and the proposed system

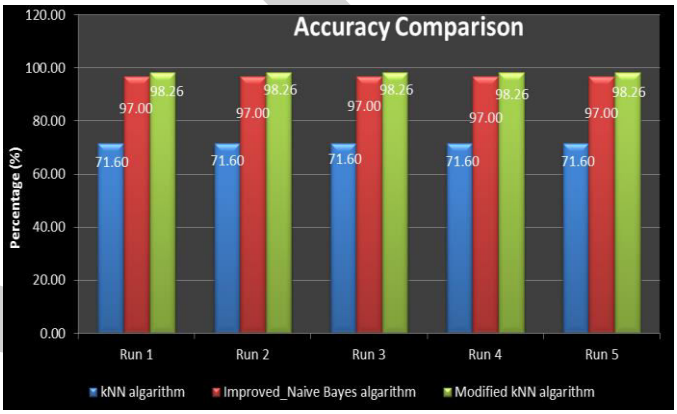

Figure 3a: Performance analysis of Accuracy based on five different run cases

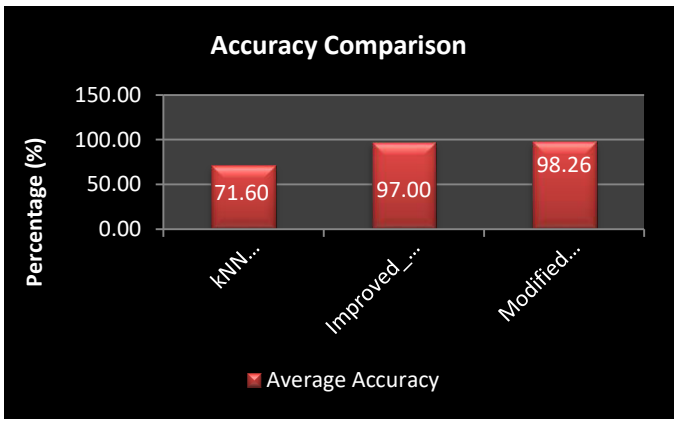

Figure 3b: Performance analysis on the basis of Accuracy

Figure 3 above, shows a graph of the existing and proposed algorithms performance analysis on the basis of Accuracy comparison. K-NN algorithm has 71.60%, Improved Naïve Bayes algorithm having 97.00% while Modified K-NN algorithm 98.25%. In this case the highest value signifies the best performing algorithm in terms of the accuracy of classified data. The proposed Modified K-NN algorithm has shown to have performed better than the existing improved naïve Bayes algorithm.

Test Case 3: Encryption time Comparison of the Classified Data

Table 4 below shows the results of five different simulated test cases for both the existing and the proposed system. The average encryption time of the different algorithms is used for the comparative analysis.

Table 3: Encryption time Comparison

	KNN		Improved Naïve Bayes		Modified KNN	
Test Case	Sensitive (RSA)	Non-Sensitive (AES)	Sensitive (RSA)	Non-Sensitive (AES)	Sensitive (RSA)	Non-Sensitive (AES)
Run 1	159210.00	2406.00	134505.00	2218.00	134112.00	2218.00
Run 2	146250.00	2360.00	150087.00	3459.00	142339.00	2360.00
Run 3	151285.00	3813.00	152201.00	3359.00	154431.00	2625.00
Run 4	139723.00	2281.00	148942.00	2219.00	150485.00	2453.00
Run 5	161124.00	3140.00	151570.00	2656.00	147097.00	3626.00
Total	**757592.00**	**14000.00**	**737305.00**	**13911.00**	**728464.00**	**13282.00**
Average Encryption Time	**151518.40**	**2800.00**	**147461.00**	**2782.20**	**145692.80**	**2656.40**

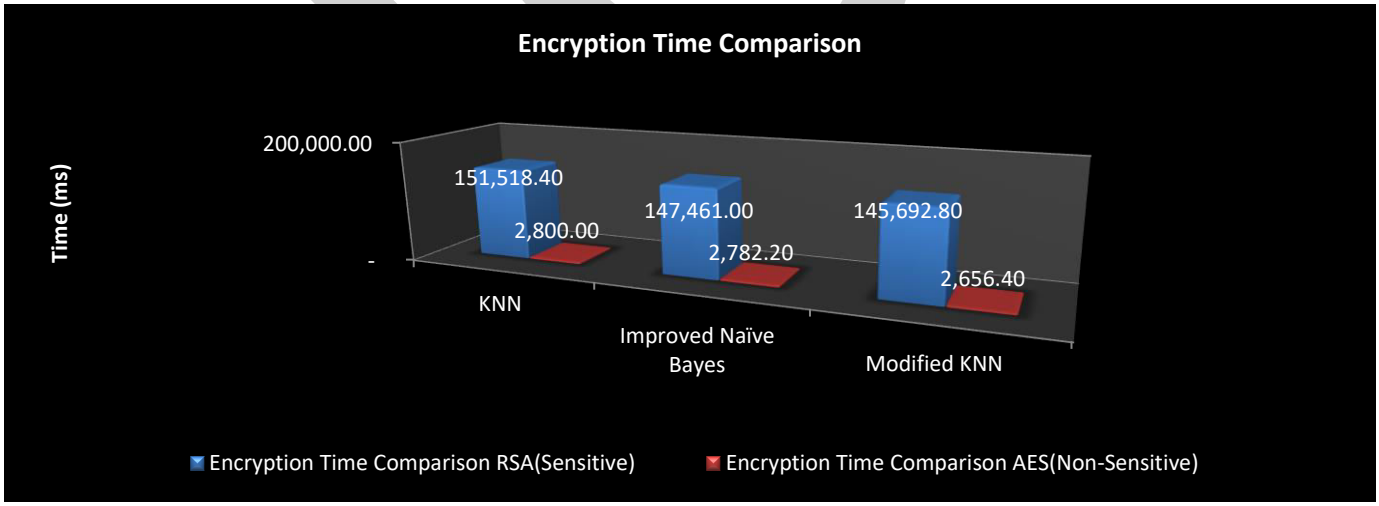

Figure 4: Performance analysis of Encryption time base on Sensitive and Non-Sensitive data

Figure 4 above reveals a graph of the existing and proposed algorithms performance analysis for encryption time comparison base on RSA algorithm for encrypting sensitive data and AES algorithm for encrypting non-Sensitive data. For K-NN algorithm RSA has 151518.40ms against AES algorithm with 2800ms. Improved Naïve bayes algorithm has RSA encryption algorithm as 147462.40ms against AES

algorithm with 2782.20ms. The Modified K-NN algorithm has 145692.80ms for RSA algorithm while AES algorithm has 2656.40ms. In this scenario, the lowest value signifies the best performing algorithm. The proposed Modified K-NN algorithm has shown to have performed better than the existing Improved Naïve Bayes algorithm in terms of RSA algorithm for encrypting sensitive data and AES algorithm for encrypting non-sensitive data.

Test Case 4: Decryption time Comparison of the Classified Data

Table 5 below shows the results of five different simulated test cases for both the existing and the proposed system. The average encryption time of the different algorithms is used for the comparative analysis.

Table 4: Decryption time comparison

	KNN		Improved Naïve Bayes		Modified KNN	
Test Case	Sensitive (RSA)	Non-Sensitive (AES)	Sensitive (RSA)	Non-Sensitive (AES)	Sensitive (RSA)	Non-Sensitive (AES)
Run 1	40279.00	2063.00	36654.00	1110.00	36298.00	937.00
Run 2	36853.00	1234.00	36830.00	1187.00	36861.00	1031.00
Run 3	36704.00	1140.00	37142.00	930.00	36298.00	953.00
Run 4	36463.00	1204.00	36470.00	1187.00	36650.00	953.00
Run 5	36854.00	1016.00	37494.00	938.00	36533.00	953.00
Total	**187153.00**	**6657.00**	**184590.00**	**5352.00**	**182640.00**	**4827.00**
Average Decryption Time	**37430.60**	**1331.40**	**36918.00**	**1070.40**	**36528.00**	**965.40**

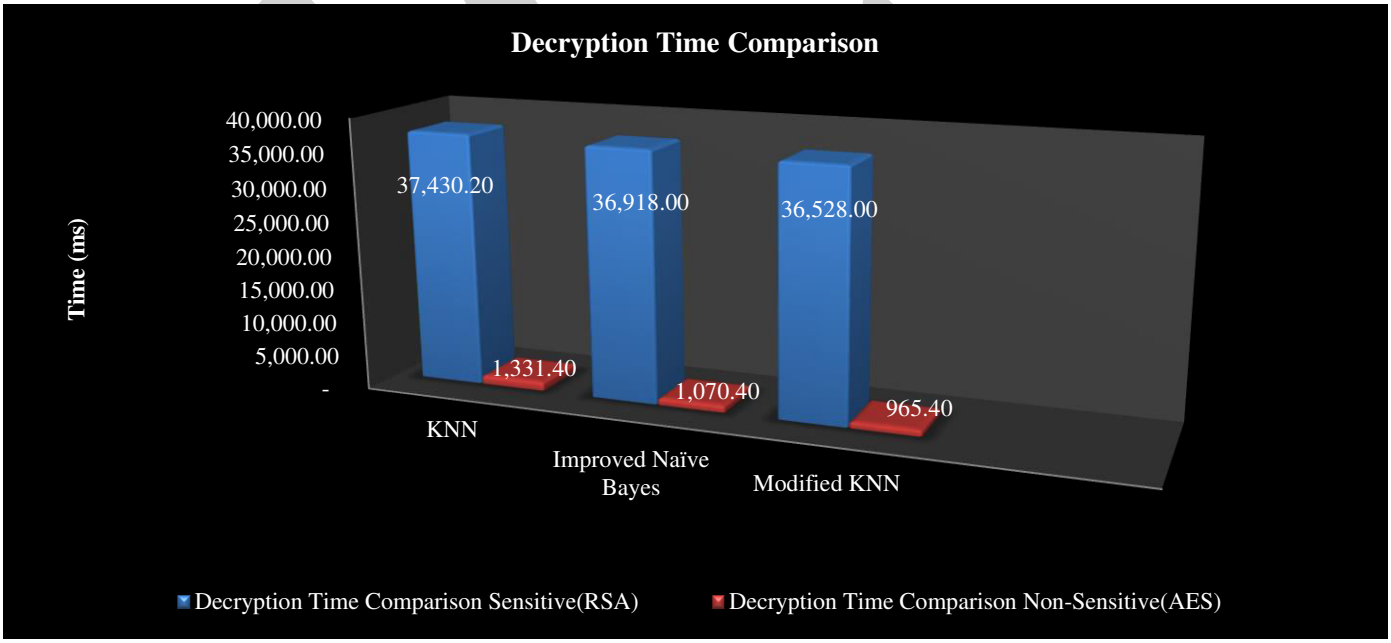

Figure 5: Performance analysis of decryption time base on Sensitive and Non-Sensitive data

Figure 5 above, shows the graphical representation of the existing and proposed approaches performance analysis for decryption time comparison with RSA algorithm for encrypting sensitive data and AES algorithm for encrypting non-sensitive data. In this scenario, the lowest value signifies the best performing algorithm. The proposed Modified For K-NN algorithm RSA has 37430.20ms and AES

algorithm with 1331.40ms. Improved Naïve Bayes algorithm has RSA encryption algorithm as 36918.00ms with AES algorithm having 1070.40ms. The Modified K-NN algorithm has 36528.00ms for RSA algorithm and AES algorithm has 965.40ms. K-NN algorithm has shown to have performed better than the existing improved naïve Bayes algorithm.

V. DISCUSSION OF RESULTS

The results obtained from the experimental performance analysis for both the existing system (which compared K-NN with Improved Naïve Bayes algorithms) and the proposed system (which compared Improved Naïve Bayes algorithm with the Modified K-NN algorithm) has it that, classification time comparison of different algorithms and the accuracy of the classified data illustrated in Figure 2, and Figure 3. The encryption and decryption time comparison is also given in the following Figure 4 and figure 5. The comparative performance analysis between Improved Naïve Bayes algorithm and Modified K-NN algorithm in terms of data classification time, accuracy of classified data, encryption and decryption with different cryptographic techniques were illustrated in these figures which shows the performance analysis of the proposed system with existing system. It is clearly analyzed and deduced from the performance graphs that the proposed methodology is better than the previous method.

Data classification time comparison illustrated in Figure 2 shows that Improved Naïve Bayes algorithm has 665.60ms and Modified K-NN is having 600.00ms. That is to say that, the proposed algorithm took less time in classifying the data than the improved naïve Bayes algorithm.

Accuracy comparison of data classification algorithms in figure 3 shows Improved Naïve Bayes algorithm and Modified K-NN algorithm having accuracy of 98.26% and improved naïve Bayes is having 97.00%. i.e. proposed algorithm has classified data more correctly.

Likewise, Figure 4 and 5 shows an enhanced encryption time and decryption time results compared to the existing approach with Improved Naïve Bayes algorithm having 147,461.00ms (RSA algorithm) with 2,782.20ms (AES algorithm) and Modified K-NN having 145,692.80ms and 2,656.40ms encryption time comparison of RSA and AES algorithms respectively. While decryption time comparison for Improved Naïve Bayes is 36,918.00ms and 1,070.00ms with Modified K-NN having 36,528.00ms and 965.40ms for RSA and AES algorithm respectively. i.e the proposed algorithm took less time to encrypt and decrypt data than previous approach.

Therefore, it can be deduced that classifying data in cloud according to its sensitivity and security needs using machine learning algorithm can reduce encryption time as purported in the proposed methodology.

Similarly, the above performance analysis shows that the proposed methodology performs significantly betters in respect to data classification time, accuracy of the classified data, encryption time and decryption time using different cryptographic techniques.

VI. CONCLUSION AND FUTURE RESEARCH

The increase in data processing in recent times has created the need to provide a platform that can accommodate the large variety of data and make them available in different location at the same time. Cloud computing is the framework that is used today to achieve this aim. The major concern with cloud computing is the security challenges. Even though, security approaches were provided using cryptography, steganography, watermarking etc. the data stored in the cloud are not all attracting the same level of protection or security. Therefore, the need to improve on the security of the classified data stored on the cloud in order to protect and identified unauthorized access on the data is vital. This work proposed an enhanced security technique on classified data in cloud using cryptography and digital watermarking technique.

The developed system has been experimented and simulated in a designed cloud simulation environment using cloudsim simulator and java developmental toolkits with Netbeans IDE. The performance analysis results depicts that the proposed technique is more relevant than storing data without deciding the security needs of the data.

Also, the result shows that Modified k-NN classification techniques work better than improved naïve Bayes technique in respect to both data classification and accuracy of the classified data. Similarly, result analysis using different security techniques to compare the encryption time and decryption time of these algorithms also shows that the security of the proposed work is stronger, efficient and robust.

In future, we recommend that other security techniques be exploits to regulate un-authorized access to the data store in the cloud. Also there is need to improved and ensure that the quality of the image cover used before and after concealing the data is recovered or maintained without distortion.

REFERENCE

[1] I. A. Adamu and B. Souley, "An Enhanced Cloud Based Security System Using RSA as Digital Signature and Image Steganography," *International Journal of Scientific & Engineering Research*, vol. 8, no. 7, pp. 1512-1517, 2017.

[2] M Boussif, N.Aloui,& A. Cherif, "Secured cloud computing for medical data based on watermarking and encryption", *IET Networks,* pp 1-5, 2018.

[3] Chandrika &E. Dalwal "Data Security in Cloud Computing using Cryptographic Algorithms: A Review",*International Journal of Innovative Research in Computer and Communication Engineering, 7(1),* pp. 89-94, 2019

[4] Dubey, S. K., & Chandra, V. (2017). Steganography, Cryptography and Watermarking: A review. *International Journal of Innovation Research in Science, Engineering and Technology, 6*(2), pp. 2595-2599.

[5] G. Garikapati, D. Yakobu, G. Nitta and l. J. Amudhave, "AN ANALYSIS OF CLOUD DATA SECURITY ISSUES AND MECHANISMS," *International Journal of Pure and Applied Mathematics*, vol. 116, no. 6, pp. 141-147, 2017.

[6] S. Gunavathy& C. Meena, "A Survey: Data Security in Cloud Using Cryptography and Steganography", *International Research Journal of Engineering and Technology, 6(5) pp 6792-6797,* 2019.

[7] O. Harfoushi, B. Alfawwaz, N. A. Ghatasheh, R. Obiedat, M. M. Abu-Faraj and H. Faris, "Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review," *Communications and Network*, vol. 6, pp. 15-21, 2014.

[8] K. B. Hari, S. Kiran, G. Murali and K. P. Reddy, "Security Issues in Services Model of Cloud Computing", *International Conference on Computational Science*, pp. 246-251, 2016.

[9] B. Jagadeesh, & K. L. Reddy, "Image Security using Digital Image and Visual Cryptography Techniques",*International Journal of Innovative Technology and Exploring Engineering, 9(4), pp. 2386-2391, 2020*

[10] J. Kaur, & S. Sharma, "HESSIS: Hybrid Encryption Scheme for Secure Image Sharingin a Cloud Environment", *Springer*, pp. 204-216, 2019.

[11] K.Kaur, &V.Zandu, "A Secure Data Classification Model for achieving Data Confidentiality and Integrity in Cloud Environment",*International Journal on Computer Science and Engineering, 8*(9), pp 362-369, 2016.

[12] M. Kaur, S. Baghla and S. Kumar, "A Review on Watermarking of Digital Images," International Journal of Advances in Science Engineering and Technology, vol. 3, no. 3, pp. 149-153, 2015.

[13] N. Khajanchi, & V. Nagrale "To Apply Watermarking Technique in Cloud Computing To Enhance Cloud Data Security",*International Journal of Scientific Development and Research, 4(7), pp. 237-244,*2019

[14] B. H. Krishna, S. Kiranb, G. Muralia and R. P. K. Reddy, "Security Issues In Service Model Of Cloud Computing Environment," *in International Conference on Computational Science*, pp. 246 – 251,2016.

[15] M. Marwan, A. Kartit, & H. Ouahmane, " Security Enhancement in Healthcare Cloud using Machine Learning", *Procedia Computer Science* 127 (2018), pp 388–397, 2018

[16] E. Mehraeen, M. Ghazisaeedi, J. Farzi and S. Mirshekari, "Security Challenges in Healthcare Cloud Computing: A Systematic Review," *Global Journal of Health Science*, vol. 9, no. 3, pp. 157-166, 2017.

[17] P. More, K. Temgire, P. Kamble and D. Chavan, "A Survey: Data Security in Cloud Computing Based on RSA," *International Engineering Research Journa,* vol. 2, no. 5, pp. 1968-1970, 2016.

[18] R. Patel and S. Dehariya, "Secure Model for Cloud Computing by using Data Classification Methodology," *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 4, no. 12, pp. 21036-21045, 2016.

[19] P. Ratha, D. Swain, B. Paikaray, & S. Sahoo, "An optimized encryption technique using an arbitrary matrix with probabilistic encryption", *3rd International Conference on Recent Trends in Computing 2015*. Elsevier B.V. pp. 1235-1241, 2015.

[20] M.O.Rahman,M.K. Hossen, G.Morsad, A.C. Roy, & S.A. Chowdhury, "An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E - LSB Encoding Technique",*IJCSNS International Journal of Computer Science and Network Security,* (18)9, pp. 85-93, 2018.

[21] S. Ramalakshmi and J. Rexy, "Enhancing Cloud Security with Automatic Data Classification and Appropriate Encryption Algorithms," *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 5, no. 1, pp. 1027-1032, 2017.

[22] G. Rathi, M. Abinaya, M. Deepika and T. Kavyasri, "Healthcare Data Security in Cloud Computing," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 3, no. 3, pp. 1807-1815, 2017

[23] M. A. Razzaq, M. A. Baig, R. A. Shaikh and A. A. Memon, "Digital Image Security: Fusion of Encryption, Steganography and Watermarking," *International Journal of Advance Computer Science and Application*, vol. 8, no. 5, pp. 224-228, 2017.

[24] H. M. Said, I. E. Emary, B. A. Alyoubi and A. A. Alyoubi, "Application of Intelligent Data Mining Approach in Securing the Cloud Computing," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 9, pp. 151-159, 2016.

[25] M. S.Sarma, Y.Srinivas, M.Abhiram,M. S.Prasanthi, &M.S.Ramya, "KNN File Classification for Securing Cloud Infrastructure",*IEEE International Conference On Recent Trends In Electronics Information & Communication Technology*. India: IEEE. pp. 5-9 2017.

[26] P.Sawle,&T.Baraskar, "Survey on Data Classification and Data Encryption Techniques Used in Cloud Computing",*International Journal of Computer Applications, 135*(12), pp 35-40, 2016.

[27] R. Shaikh and M. Sasikumarb, "Trust Model for Measuring Security Strength of Cloud Computing Service," *in International Conference on Advanced Computing Technologies and Applications*, pp. 380-389, 2015.

[28] K.P. Singh, V. Rishiwal, & P. Kumar, "Classification of Data to Enhance Data Security in Cloud Computing", IEEE. pp. 1-5, 2018

[29] T. Tamanna and K. Rajeev, "Secure Cloud Model Using Classification and Cryptography," *International Journal of Computer Application*, vol. 159, no. 6, pp. 8-13, 2017.

[30] L. Tawalbeh, N. S, Darwazeh, R. S, Al-Qassas and F. AlDosari, "A Secure Cloud Computing Model based on Data Classification," *Procedia Computer Science*, pp. 1153-1159, 2015.

[31] F. Yahya, R. J. Walters and G. B. Wills, "Protecting Data in Personal Cloud Storage with Security Classifications," *in Science and Information Conference, London*, pp. 838-843, 2015