Performance of Symmetric and Asymmetric Encryption Techniques for Attribute Based Encryption

Devendrasinh Vashi, H B Bhadka, Kuntal Patel, Sanjay Garg

ABSTRACT: The objective of this research article is to study performance of the the symmetric and asymmetric encryption based on the attributed encryption. In the current scenario, to protect the data in the distributed data base is the challenging task. Mainly to provide the privacy based on the specific parameter like attributed based encryption. In this algorithm dataset is provided to do the encryption for the selected sensitive attribute. Them for each symmetric and asymmetric encryption techniques encryption execution time and memory occupied after encryption is observed for ten different dataset. In the experiment and result analysis, each encryption techniques was discussed based on the comparion of encryption time and memory occupied after encryption. Result shows that RC2 encryption is less costlier as compare to AES, 3DES, Rijndael and RSA encryption. Result also indicates that 3DES and RC2 are almost need same encryption time and less costlier as compare to RSA, AES and Rijndael encryption and RSA encryption is more costlier as compare to AES, 3DES, Rijndael and RC2 encryption.

***Keywords** : privacy preserving, data, Data Mining, encryption, PPDM, Symmetric encryption, Asymmetric encryption.*

I. INTRODUCTION

In current scenario, database is increasing day by day in all the sector. Some organizations are trying to do find out some useful information through data mining from these database. Sometimes identity of the person may reveal. So people are trying the encrypt some part of the data so during data mining those data will not be disclosed to third party. This process is called privacy preserving data mining [7] (PPDM) .

Encryption techniques is the only solution through which information can be secured. There two types of encryption techniques which are widely used in the different applications. One is symmetric encryption and second kind is asymmetric encryption. Mainly AES, 3DES, Rijndael, RC2 and RSA encryption techniques are used in the majority of the application to secure the information.

Revised Manuscript Received on November 15, 2019

Devendrasinh Vashi, Computer Science Department, Nirma University, Ahmedabad, India. Email: devendra.vashi@gmail.com

Dr. H B Bhadka, Faculty of Computer Science, C U Shah University, Wadhwan, India, harshad.bhadka@yahoo.com

Dr. Kuntal Patel, School of Computer Studies, Ahmedabad University, Ahmedabad, India, kuntal.patel@ahduni.edu.in

Dr. Sanjay Garg, Computer Science Department, Nirma University, Ahmedabad, India. Email: sgarg@nirmauni.ac.in

II. ALGORITHM

In the implemented work symmetric encryption [10] approach algorithm is implemented with symmetric [11] and asymmetric encryption on uploaded excel sheet for the selected attributes which might reveal the privacy [1].

Step-1: Start
Step-2: Collect the data for creating dataset in excel sheet
Step-3: Upload the excel sheet in the application which will convert the database in to sql server compatible data.
Step-4: Select the sensitive attributes (Name, Gender, Address 2(City)(Home), Mobile No, E-Mail ID, Salary and Pan Card Number from each data set to encrypt.
Step-5 : Implement the AES, 3DES, Rijndael, RC2 and RSA encryption for the attribute which is t be encrypted in th table.
Step-6: Observer the table size before and after encryption for 10 different datasize file.
Step-7: Download the file with encrypted data which for sharing with third party for Privacy Preseving Data Mining.
Step-8 : Stop

III. DATABASE ATTRIBUTES

Following 23 attributes were considered during implementation of the proposed algorithm:

Timestamp
Name
Gender
Date of birth
Blood Group
Disability
Pan card Number
Diseases
Medication & allergies
Mobile No.
E-mail ID
Salary

Nationality
Education
Marital Status
Address 1(Street) [Home]
Address 2(City)[Home]
Address 3(State) [Home]
Address 1(Street)[Work Space]
Address 2(City)[Work Space]
Address 3(State)[Work Space]
Doctor Name
Date & Time of visit

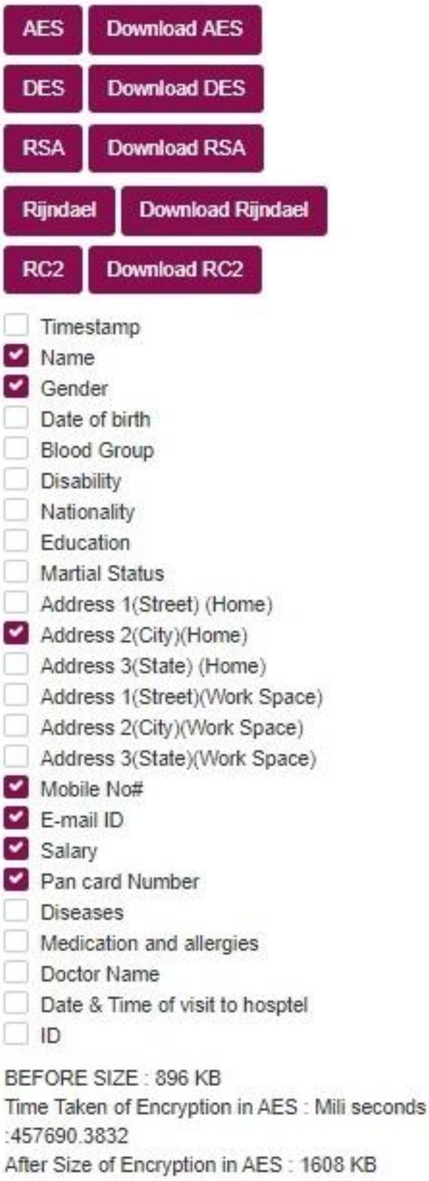
IV. EXPERIMENT AND RESULT ANALYSIS

In the implementation of AES, 3DES, Rijndael, RC2 and RSA encryption ten excel file was prepared of 100 kb, 200 kb, 300, kb, 400 kb, 500 kb, 600 kb, 700 kb, 800 kb, 900 kb, and 1000 kb. Each sheet contains the data of different kinds of sensitive attributes [6][8]. Initially, 100 kb file is used. The selection of attributes was based on the survey from different age people. Then on the given 100 kb file for the selected sensitive attributes, i.e. Name, Gender, Address 2(City)(Home), Mobile No, E-Mail ID, Salary, Pan Card Number, AES symmetric encryption technique implemented and noted the encryption time and memory required for each encryption. Then one by one file size is increased by 100 kb for each encryption and noted the encryption time and memory used for the same selected sensitive attributes. The same process is repeated for 3DES, Rijndael, RC2 and RSA [2] respectively as per table-I to table-V.

At the end as per the proposed algorithm for table-I contains the data of AES encryption, table-II contains the data of 3DES encryption, table-III contains the data of Rijndael encryption, table-IV contains the data of RC2 encryption and table-V contains the data of RSA encryption techniques. Encryption time and memory before and after execution time for 10 different size database was observed.

Fig 2 to Fig 6 depict that execution time increase with respect to file size increased for the implemented encryption techniques. And Fig.7. shows the results Comparison of AES, 3DES, Rijndael, RC2 and RSA [3][9] technique based on execution time.

Fig 8 to Fig 12 depict that memory occupied after encryption increased with respect to file size increase for the implemented encryption techniques. And Fig.13. shows the results Comparison of AES, 3DES, Rijndael, RC2 and RSA technique [4] [5] based on memory occupied after encryption



□ Timestamp
☑ Name
☑ Gender
□ Date of birth
□ Blood Group
□ Disability
□ Nationality
□ Education
□ Martial Status
□ Address 1(Street) (Home)
☑ Address 2(City)(Home)
□ Address 3(State) (Home)
□ Address 1(Street)(Work Space)
□ Address 2(City)(Work Space)
□ Address 3(State)(Work Space)
☑ Mobile No#
☑ E-mail ID
☑ Salary
☑ Pan card Number
□ Diseases
□ Medication and allergies
□ Doctor Name
□ Date & Time of visit to hosptel
□ ID

BEFORE SIZE : 896 KB
Time Taken of Encryption in AES : Mili seconds
:457690.3832
After Size of Encryption in AES : 1608 KB

Fig. 1: 3DESign of attribute selection for the symmetric & asymmetric encryption

Table- I: Execution time and memory occupied of different size dataset with AES technique

File name with data size (kb).	**Table size before encryption (kb)**	**Encryption time to Table (milliseconds)**	**Table size after encryption (kb)**
Sensitive data 1.xlsx (100)	432	194841.6345	792
Sensitive data 2.xlsx (200)	896	422397.1474	1608
Sensitive data 3.xlsx (300)	1064	754157.5066	2288
Sensitive data 4.xlsx (400)	1824	878551.8027	3232
Sensitive data 5.xlsx (500)	2288	1067189.4808	4024
Sensitive data 6.xlsx (600)	2736	1312235.4215	4816
Sensitive data 7.xlsx (700)	3120	1599662.8853	5616
Sensitive data 8.xlsx (800)	3480	1958078.8976	6368
Sensitive data 9.xlsx (900)	4000	2167277.419	7120
Sensitive data 10.xlsx (1000)	4416	2486791.9799	7944

Table- II: Execution time and memory occupied of different size dataset with 3DES technique

File name with data size (kb).	**Table size before encryption (kb)**	**Encryption time to Table (milliseconds)**	**Table size after encryption (kb)**
Sensitive data 1.xlsx (100)	432	11804.6417	752
Sensitive data 2.xlsx (200)	896	41490.2738	1512
Sensitive data 3.xlsx (300)	1064	141784.5123	1976
Sensitive data 4.xlsx (400)	1824	146550.8097	3024
Sensitive data 5.xlsx (500)	2288	201515.4247	3792
Sensitive data 6.xlsx (600)	2736	280816.6168	4512
Sensitive data 7.xlsx (700)	3120	417416.8003	5200
Sensitive data 8.xlsx (800)	3480	554070.3787	5832
Sensitive data 9.xlsx (900)	4000	606566.0707	6648
Sensitive data 10.xlsx (1000)	4416	778786.8911	7344

Table- III: Execution time and memory occupied of different size dataset with Rijndael technique

File name with data size (kb).	Table size before encryption (kb)	Encryption time to Table (milliseconds)	Table size after encryption (kb)
Sensitive data 1.xlsx (100)	432	11098.8138	792
Sensitive data 2.xlsx (200)	896	30956.6644	1608
Sensitive data 3.xlsx (300)	1064	131389.6595	2304
Sensitive data 4.xlsx (400)	1824	134382.5819	3224
Sensitive data 5.xlsx (500)	2288	192659.5592	4024
Sensitive data 6.xlsx (600)	2736	268350.7796	4816
Sensitive data 7.xlsx (700)	3120	411422.9459	5616
Sensitive data 8.xlsx (800)	3480	555403.4911	6344
Sensitive data 9.xlsx (900)	4000	611341.6039	7152
Sensitive data 10.xlsx (1000)	4416	779028.4162	7952

Table- IV: Execution time and memory occupied of different size dataset with RC2 technique

File name with data size (kb).	Table size before encryption (kb)	Encryption time to Table (milliseconds)	Table size after encryption (kb)
Sensitive data 1.xlsx (100)	432	16311.8323	752
Sensitive data 2.xlsx (200)	896	48831.4074	1512
Sensitive data 3.xlsx (300)	1064	135291.4238	1960
Sensitive data 4.xlsx (400)	1824	161633.6996	3032
Sensitive data 5.xlsx (500)	2288	244855.7505	3792
Sensitive data 6.xlsx (600)	2736	287984.1321	4512
Sensitive data 7.xlsx (700)	3120	350023.5683	5200
Sensitive data 8.xlsx (800)	3480	472355.3075	5848
Sensitive data 9.xlsx (900)	4000	537490.4692	6656
Sensitive data 10.xlsx (1000)	4416	660156.5627	7336

Table- V: Execution time and memory occupied of different size dataset with RSA technique

File name with data size (kb).	Table size before encryption (kb)	Encryption time to Table (milliseconds)	Table size after encryption (kb)
Sensitive data 1.xlsx (100)	432	168076.7119	2632
Sensitive data 2.xlsx (200)	896	379964.5951	5592
Sensitive data 3.xlsx (300)	1064	823985.3688	10416
Sensitive data 4.xlsx (400)	1824	862798.1676	11544
Sensitive data 5.xlsx (500)	2288	1106278.8166	14472
Sensitive data 6.xlsx (600)	2736	1400268.4375	17424
Sensitive data 7.xlsx (700)	3120	1808942.3922	20808
Sensitive data 8.xlsx (800)	3480	2114358.7855	23992
Sensitive data 9.xlsx (900)	4000	2340048.2433	26520
Sensitive data 10.xlsx (1000)	4416	2723930.2683	29624

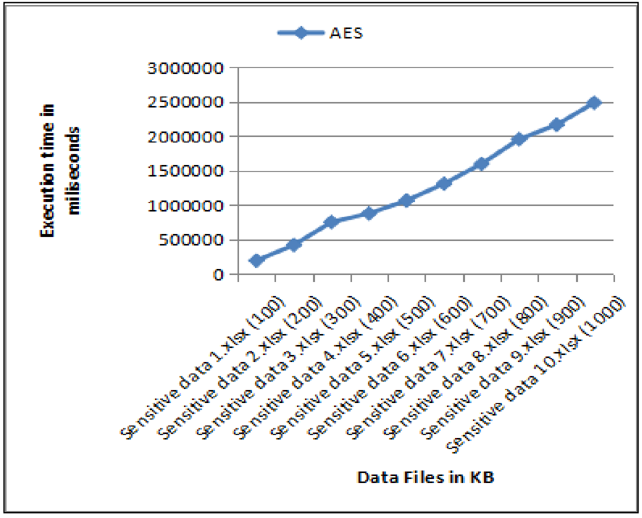


Fig. 2 Observation of AES technique based on execution time

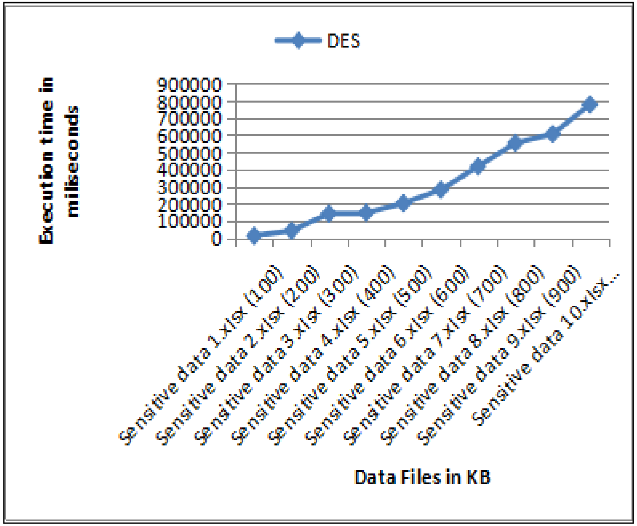


Fig. 3 Observation of 3DES technique based on execution time

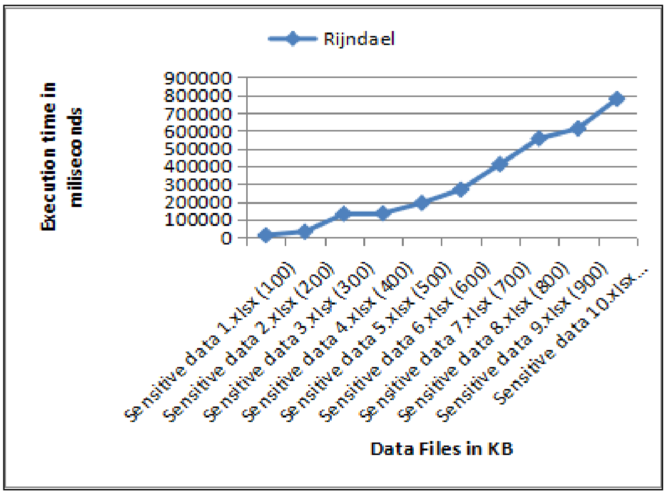


Fig. 4 Observation of Rijndael technique based on execution time

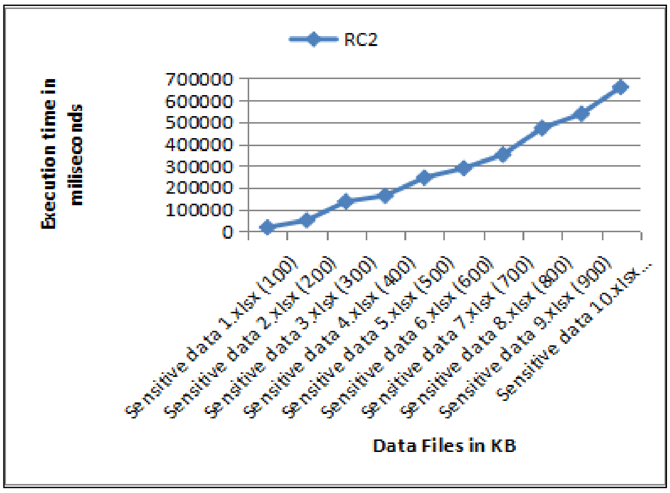


Fig. 5 Observation of RC2 technique based on execution time

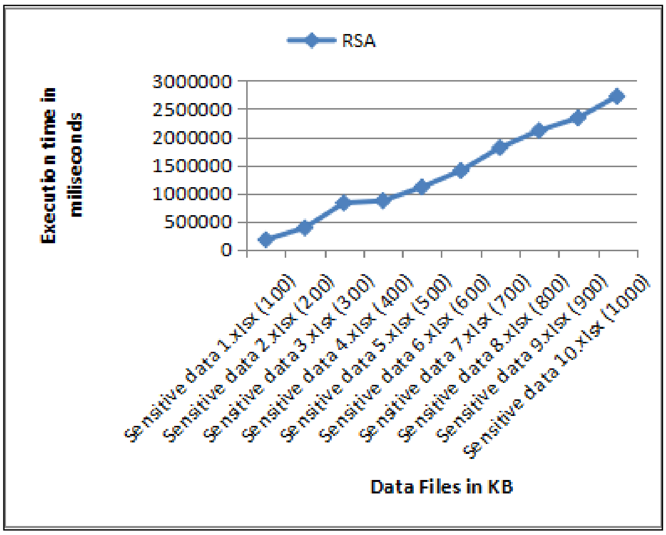


Fig. 6 Observation of using RSA technique based on execution time

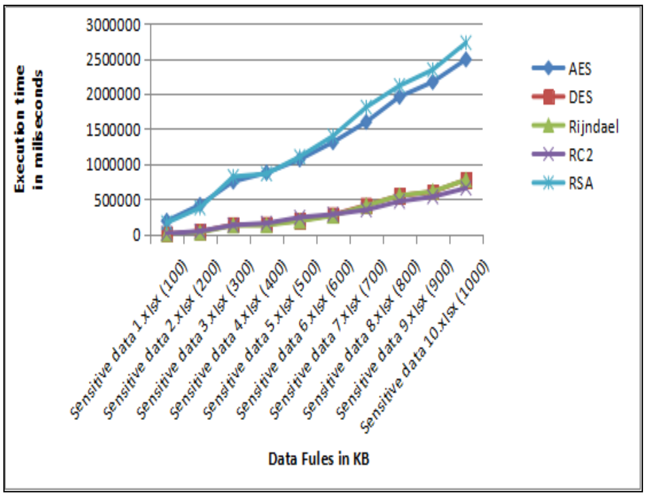


Fig. 7 Observation of AES, 3DES, Rijndael, RC2 and RSA technique based on execution time

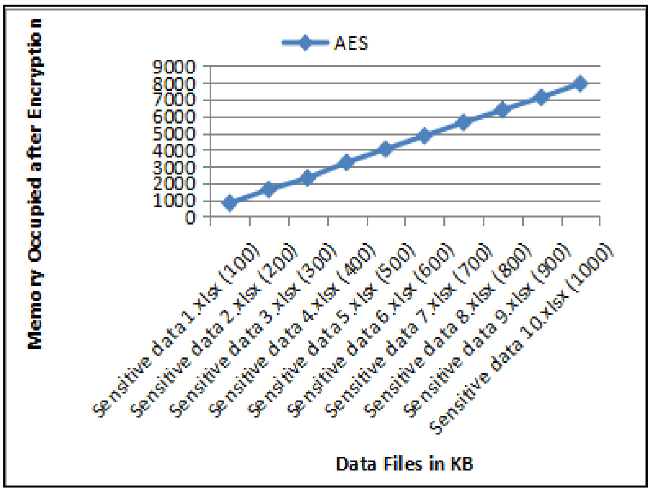


Fig. 8 Observation of AES based on memory occupied after encryption

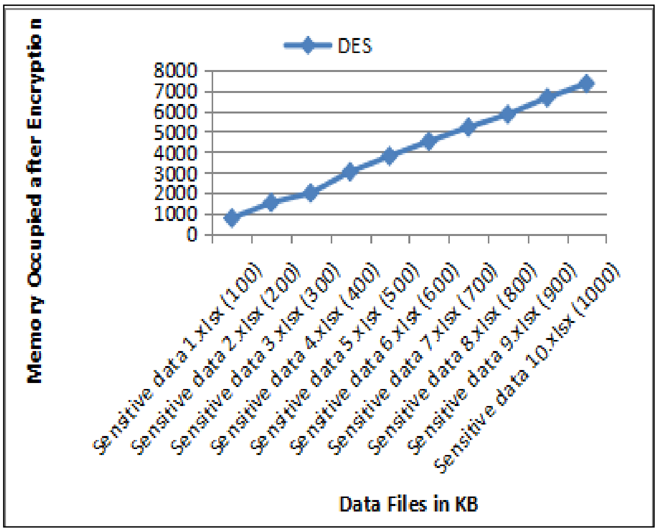


Fig. 9 Observation of 3DES technique based on memory occupied after encryption

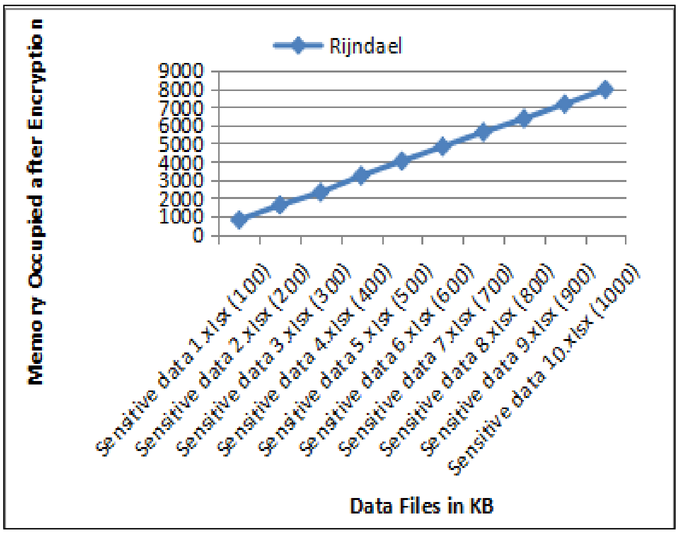


Fig. 10 Observation of Rijndael technique based on memory occupied after encryption

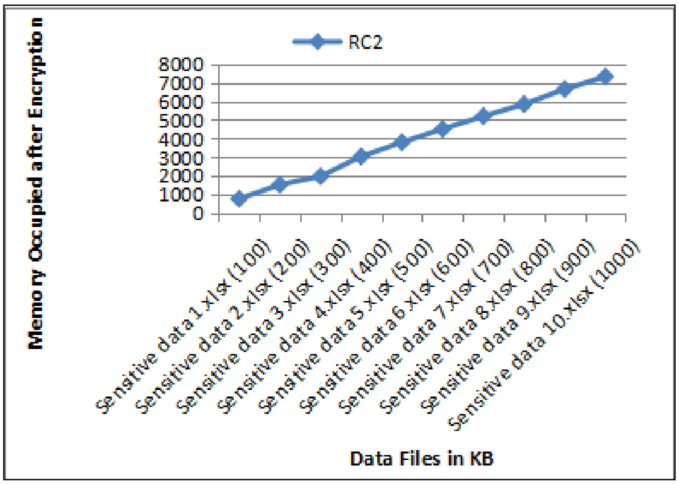


Fig. 11 Observation of RC2 technique based on memory occupied after encryption

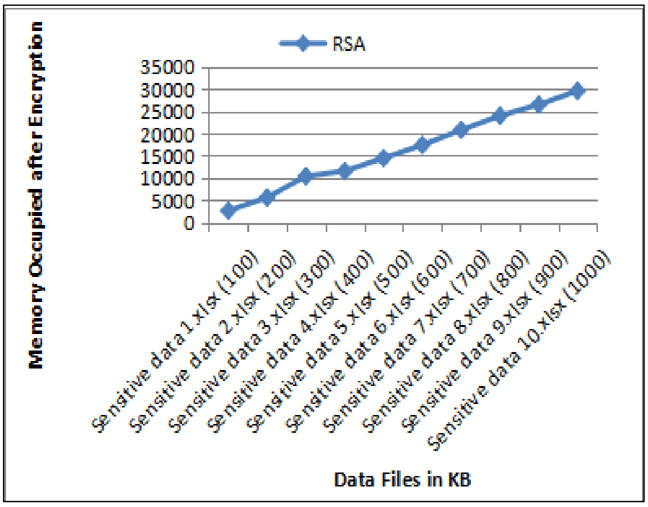


Fig. 12 Observation of RSA technique based on memory occupied after encryption

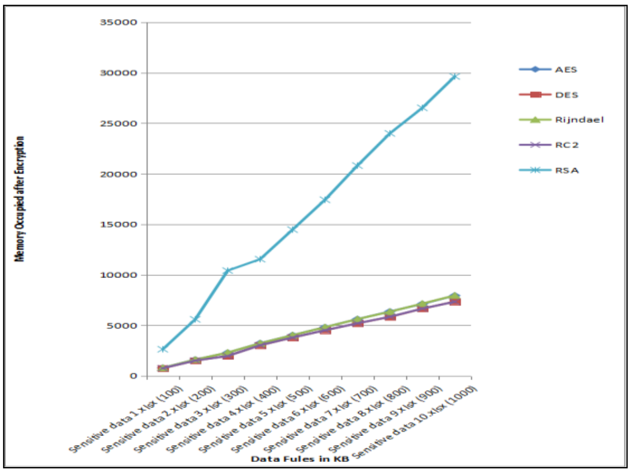


Fig. 13 Observation of AES, 3DES, Rijndael, RC2 and RSA technique based on memory occupied after encryption

V. CONCLUSION

Following observation is made with respect to the encryption time for the attributed based encryption:

1. The experimental data of table-V and graphs of Fig. 7 indicates that RSA encryption is more costlier as compare to AES, 3DES, Rijndael and RC2 encryption .
2. The experimental data of table-I and graphs of Fig. 7 indicates that AES encryption is less costlier than RSA encryption.
3. The experimental data of table-II, table-III and graphs of Fig. 7 indicates that Rijndael and 3DES are almost need same encryption time and less costlier as compare to RSA and AES encryption.
4. Lastly, the experimental data of table-IV and graphs of Fig. 7 indicates that RC2 encryption is less costlier as compare to AES, 3DES, Rijndael and RSA encryption.

Following observation is made with respect to the memory occupied after encryption for the attributed based encryption:

1. The experimental data of table-V and graphs of Fig. 13 indicates that RSA encryption is more costlier as compare to AES, 3DES, Rijndael and RC2 encryption .
2. The experimental data of table-I, table-III and graphs of Fig. 13 indicates that AES and Rijndael are almost need same encryption time and less costlier as compare to RSA encryption.

3. Lastly, the experimental data of table-II, table-IV and graphs of Fig. 13 indicates that 3DES and RC2 are almost need same encryption time and less costlier as compare to RSA, AES and Rijndael encryption.

so such attributed based encryption with symmetric encryption techniques are more suitable and less costlier than asymmetric encryption technique in privacy-preserving data mining.

REFERENCES

1. Rahulamathavan, Yogachandran, et al. "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption." 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). IEEE, 2017.
2. Patil, Priyadarshini, et al. "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish." Procedia Computer Science 78 (2016): 617-624.

3. Singh, Gurpreet. "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security." International Journal of Computer Applications 67.19 (2013).
4. Verma, Harsh Kumar, and Ravindra Kumar Singh. "Performance analysis of RC6, Twofish and Rijndael block cipher algorithms." International Journal of Computer Applications 42.16 (2012): 1-7.
5. Gunasundari, T., and K. Elangovan. "A Comparative Survey on Symmetric Key Encryption Algorithms." International Journal of Computer Science and Mobile Applications 2.2 (2014): 78-83.
6. Devendra I Vashi et al., Critical Study and Analysis for Deciding Sensitive and Non-Sensitive Attributes of Medical Healthcare dataset Through Survey and Using Association Rule Mining. Int J Recent Sci Res. 8(5), pp. 17218-17222.
7. Devendra I Vashi et al (2017), "Challenges & Opportunities in Privacy Preserving Data Mining for Healthcare Dataset", International Conference on “Research and Innovations in Science, Engineering & Technology”, ICRISET-2017
8. Devendrasinh Vashi et al., Implementation of Attribute Based Symmetric Encryption Through Vertically Partitioned Data in PPDM, International Journal of Engineering and Advanced Technology, 8(6), pp. 5384-5390.
9. Kuntal Patel, “Performance analysis of AES, 3DES and Blowfish cryptographic algorithms on small and large data files”, International Journal of Information Technology, ISSN: 2511-2104
10. Tripathi, Ritu, and Sanjay Agrawal. "Comparative study of symmetric and asymmetric cryptography techniques." International Journal of Advance Foundation and Research in Computer (IJAFRC) 1.6 (2014): 68-76.
11. Agrawal, Monika, and Pradeep Mishra. "A comparative survey on symmetric key encryption techniques." International Journal on Computer Science and Engineering 4.5 (2012): 877.

AUTHORS PROFILE

Prof Devendrasinh Vashi is working as an Assistant Professor in the Computer Science and Engineering Department. He has more than 13 years of teaching experience. Prof Vashi received his MCA degree from the Visvesvaraya Technological University, Belgaum. He has published two research article in reputed journal. He has also presented two research papers in international conference. He has organized one Shor Term Training Programme successfully. He is currently pursuing his doctoral studies from C U Shah University, Surendranagar in the field of Privacy Preserving Data Mining.

Dr. H B Bhadka is working as Dean at Faculty of Computer Science, C. U. Shah University, Wadhwan City. Gujarat, India. He has completed his Ph. D. in 2009, from Saurashtra University. Currently working as Dean of Faculty of Computer Science, C. U. Shah University, Surendranagar. Working as Head of Institute since 2006 at CCMCA. Published 70+ Research Papers, attended many conferences, attended many workshops. He has successfully supervised two PhD dissertations and is currently guiding two PhD students in the field of Data Mining, privacy preserving in data mining. He is also a reviewing the PhD thesis of his research area.

Dr. Kuntal Patel is currently working as an Assistant Professor at School of Computer Studies, Ahmedabad University. Being a researcher on "IT Standards", he has completed his Ph. D. from North Gujarat University in 2006. He has published more than 25 research papers at peer-reviewed Journals and Conferences. He is certified Cyber Security Professional. He is actively involved in Google, ACM-India and Govt. of Gujarat supported Activity Based Learning Project called CS-Pathshala. He is an editorial board member of Computer Science textbook of Gujarat Board. He is the Secretary and Professional member of Association of Computer Machinery (ACM) – Ahmedabad chapter and life time member of CSI and ISTE.

Dr Sanjay Garg is working as Professor in Computer Science and Engineering Department. He has more than 31 years of teaching experience. Dr Garg has done his BE in Computer Technology from SATI, Vidisha (Barkattullah University, Bhopal) in 1991, ME in Computer Engineering and Automation from SGISTS, Indore in 2001 and PhD in Computer Science from Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal in 2009. He has completed three funded research projects as Principal Investigator, two of them were sponsored by ISRO, under RESPOND scheme, other one by GUJCOST. Additionally two research projects sponsored by ISRO are in progress currently. He has successfully supervised six PhD dissertations and is currently guiding two PhD students in the field of Data Mining, Pattern Recognition and Image Processing.