ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

CLOUD BASED SERVER INCORPORATING ATTRIBUTE BASED ENCRYPTION (ABE) PROCESSES

A. Vinoth Kumar*, Dr. M. Anand

* Research Scholar, ECE Department, Dr.M.G.R. Educational and Research Institute University, Chennai

Professor, ECE Department, Dr.M.G.R. Educational and Research Institute University, Chennai

DOI: 10.5281/zenodo.187357

ABSTRACT

In this research, a novel technique termed as Attribute Based Encryption (ABE) Processes is proposed ,Here the cloud server is allowed to learn only the set of encrypted documents and its attributes or features, without requiring to have a knowledge about the keyword data which is unlike the traditional data encryption based systems. Significance of this research is that accessing client through server becomes easier and also client can encrypt, store and search data by their own key on server. Another significant aspect of ABE is the ease with which client's private key is associated with a set of attributes and the cipher text specifies a well-defined access policy over a universe of attributes within the system.

KEYWORDS: Encryption, Decryption, Data searching, ABE, Cloud Server.

INTRODUCTION

Normally, for storing huge volumes of data to the cloud server, the client usually employs a third party service provider that must be insulated from the transactions occurring between the client and the cloud server. Before sending to the server, the data must be encrypted as sensitive and private information may be present. This is one type of a public key encryption technique, where the secret key of the client and the cipher key depend upon attributes. The decryption takes place only when the attributes of the user key matches that of the ciphertext. Here, the server also plays an important role in assisting the clients in data searching. All the data sent back to the client for decryption may also be searched. But these methodologies are not efficient enough as for as searching the encrypted data is concerned and also the data privacy and security is also compromised.

RELATED WORKS

In this paper [1], Cloud computing is an emerging paradigm that provides various IT related services. The security and privacy are two major factors that inhibits the growth of cloud computing. Security factors are reasons behind lesser number of real times and business related cloud applications compared to consumer related cloud application. Firstly, the pros and cons of different Attribute Based encryption methods are analyzed. Secondly, a new encryption method based on Attribute Based Encryption (ABE) using hash functions, digital signature and asymmetric encryptions scheme has been proposed. The proposed algorithm is simplified yet efficient algorithm that can implemented for cloud critical application.

Attribute-based encryption (ABE) is a type of public key encryption that allows users to encrypt and decrypt messages based on user attributes. One drawback is that encryption and encryption computational costs scale with the complexity of the access policy or number of attributes. Practically, this makes encryption and decryption a possible bottleneck for some applications. In this work, we aim to mitigate this problem for ciphertext-policy ABE (CP-ABE). We introduce the server aided CP-ABE (SA-CP-ABE) system. In [2], users can precompute an intermediate ciphertext before actual encryption to improve efficiency, and stores it on its storage server. Before decryption, user can call its computing server to transform the ciphertext to the partially decrypted ciphertext. This is significant for mobile devices to save local storage resources and computational resources.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Various numbers of diverse applications that include e- payments in secure commerce and payment applications to provide security for their communications and transactions by protecting passwords has been discussed. Encryption is a fundamental tool for the protection of sensitive information. The purpose is to use encryption is privacy for preventing disclosure or confidentiality in during communications. [3] proposes a new method which is based on the Euler's Totient theorem to produce a set of numbers that encrypt the data stream and then we used our proposed method using an ECC approach to generate the signature key which is added to encrypt data before transmission and decryption operation and a signature can verify at the receiver site.

Outsourcing the data in cloud computing is exponentially generated to scale up the hardware and software resources. How to protect the outsourced sensitive data as a service is becomes a major data security challenge in cloud computing. To address these data security challenges, we propose an efficient data encryption to encrypt sensitive data before sending to the cloud server. This exploits the block level data encryption using 256 bit symmetric key with rotation. In addition, data users can reconstruct the requested data from cloud server using shared secret key. The privacy protection of outsourced data is analyzed in [4] using experiment is carried out on the repository of text files with variable size. The security and performance analysis shows that the proposed method is highly efficient than existing methods performance.

Paper [5] describes the algorithm and the developed training module with graphical user interface for encryption and decryption of texts using affine ciphers, which will be used in the course "Telecommunications Security" included as compulsory in the curriculum of the specialty

"Telecommunication Systems" for "Bachelor" educational qualification degree at the University of Ruse. The training module is implemented using MATLAB and Graphical User Interface development Environment GUIDE. The application allows selecting the language through radio-buttons and the parameters of the encryption/decryption key from a drop-down menu. It illustrates step by step the process of encryption/ decryption of the plain-text/cipher-text entered in the text field by the user, using affine ciphers. The novelty is that the algorithm for encryption /decryption of texts in English using affine ciphers is modified to be used for texts in Bulgarian, Russian or Romanian and it could be implemented in other languages (depending on the number of letters in the alphabet). The module has a possibility to display information on affine ciphers and to illustrate the principle of its operation in a separate graphical window, if desired by the user.

A novel scheme called Broadcast Searchable Keywords Encryption (BSKE) is proposed in [6] that allows searching in encrypted data without knowing a secret key. Consider Bob wants to encrypt the same data under master public key for a group of users and stores this encrypted data with Alice, Malice is one of those recipients he asks Alice using his private key whether or not she has stored encrypted data, then Alice will search in all encrypted data using the master public key, either she finds a matching then returns encrypted data to Malice or does nothing .We hopefully wish Alice will not learn anything from both encrypted data and the query. Our scheme contributes by providing fixed ciphertext O(3) which does not grow with the number of recipients , efficient revocable for users without resets security parameters and the computational cost in the cloud side only. BSKE is designed based on random oracle model and the scheme is secured against adaptive chosen keyword attack.

A novel method Ciphertext-policy attribute-based encryption (CP-ABE) which enables fine-grained access control to the encrypted data for commercial applications has been proposed in [7]. There has been significant progress in CP-ABE over the recent years because of two properties called traceability and large universe, greatly enriching the commercial applications of CP-ABE. Traceability is the ability of ABE to trace the malicious users or traitors who intentionally leak the partial or modified decryption keys for profits. Nevertheless, due to the nature of CP-ABE, it is difficult to identify the original key owner from an exposed key since the decryption privilege is shared by multiple users who have the same attributes. On the other hand, the property of large universe in ABE enlarges the practical applications by supporting flexible number of attributes. Several systems have been proposed to obtain either of the above properties. However, none of them achieve the two properties simultaneously in practice, which limits the commercial applications of CP-ABE to a certain extent. In this paper, we propose two practical large universe CP-ABE systems supporting white-box traceability. Compared with existing systems, both the two proposed systems have two advantages: 1) the number of attributes is not polynomially bounded and 2) malicious users who leak their decryption keys could be traced. Moreover, another remarkable advantage of the second proposed system is that the storage overhead for traitor tracing is constant, which are suitable for commercial applications.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Attribute Based Encryption (ABE) is a type of public encryption where decryptor can only decrypt the ciphertext if its attributes of the secret key matches the attributes of ciphertext but functionality comes at higher cost. The idea is to provide multi authority in attribute based encryption which also allows fast decryption. Multi authority concept allows any polynomial number of independent authorities to monitor attributes, distribute secret keys and decrypt the message. In this paper, a secure multi authority attribute based encryption with fast decryption scheme is proposed and designed.

In this paper [9], Attribute-based encryption (ABE) with outsourced decryption not only enables fine-grained sharing of encrypted data, but also overcomes the efficiency drawback (in terms of ciphertext size and decryption cost) of the standard ABE schemes. In particular, an ABE scheme with outsourced decryption allows a third party (e.g., a cloud server) to transform an ABE ciphertext into a (short) El Gamal-type ciphertext using a public transformation key provided by a user so that the latter can be decrypted much more efficiently than the former by the user. However, a shortcoming of the original outsourced ABE scheme is that the correctness of the cloud server's transformation cannot be verified by the user. That is, an end user could be cheated into accepting a wrong or maliciously transformed output. A security model of ABE is formalized with verifiable outsourced decryption by introducing a verification key in the output of the encryption algorithm. Then, we present an approach to convert any ABE scheme with outsourced decryption into an ABE scheme with verifiable outsourced decryption. Compared with the original outsourced ABE, our verifiable outsourced ABE neither increases the user's and the cloud server's computation costs except some non-dominant operations (e.g., hash computations) nor expands the ciphertext size except adding a hash value (which is <20 byte for 80-bit security level). We show a concrete construction based on Green et al.'s ciphertext-policy ABE scheme with outsourced decryption, and provide a detailed performance evaluation to demonstrate the advantages of our approach.

Multi-Authority Attribute-Based Encryption is a promising cryptographic technique for realizing fine-grained access control on the encrypted data in cloud computing. However, existing multi-authority based attribute encryption schemes in cloud computing generally do not take into account the attribute with weight. In [10] the concept of weight is introduced into multi-authority based attribute encryption scheme. Multi-authority based weighted attribute encryption scheme in cloud computing is proposed. The attribute authorities assign different weights to attributes according to their importance. The analysis shows that the proposed scheme is secure. Since the scheme can reflect the significance of attributes, it is more suitable for the cloud computing environment than the existing schemes.

Paper [11] mentions the advent of cloud computing, most of the data owners are outsourcing their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But sensitive data has to be encrypted before outsourcing, for protecting data privacy. However data encryption makes effective data utilization a challenging task. Traditional data utilization based keyword search on encrypted data is a difficult task. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in the cloud, it is necessary to allow keyword search request and return documents in the order of their relevance to these keyword. In this paper we proposed a system that supports multi owner keyword ranked search over the encrypted cloud data with good key management scheme. Thorough security and performance analysis show that the proposed scheme guarantees high security and practical efficiency.

In [12] a number of extended Proxy Re-Encryptions (PRE), e.g. Conditional (CPRE), identity-based PRE (IPRE) and broadcast PRE (BPRE), have been proposed for flexible applications. By incorporating CPRE, IPRE and BPRE, this paper proposes a versatile primitive referred to as conditional identity-based broadcast PRE (CIBPRE) and formalizes its semantic security. CIBPRE allows a sender to encrypt a message to multiple receivers by specifying these receivers' identities, and the sender can delegate a re-encryption key to a proxy so that he can convert the initial ciphertext into a new one to a new set of intended receivers. Moreover, the re-encryption key can be associated with a condition such that only the matching ciphertexts can be re-encrypted, which allows the original sender to enforce access control over his remote ciphertexts in a fine-grained manner. In the instantiated scheme, the initial ciphertext, the re-encrypted ciphertext and the re-encryption key are all in constant size, and the parameters to generate a re-encryption key are independent of the original receivers of any initial ciphertext.

Cloud computing is one of the emerging technology of IT industry in recent times. This new technology requires entrust the user's valuable data to the cloud server, since this cloud computing have the major disadvantage over security and privacy to the outsourced data to the server. To overcome this disadvantage several attribute-based

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

encryption (ABE) schemes are reported for the user's data file encryption and also for the access control of the outsourced data in the cloud server; however, implementing of access control policies in attribute-based encryption (ABE) is more complex. The attribute-based encryption (ABE) has two type techniques Ciphertext-Policy Attribute-Based Encryption (CPABE) and Key Policy Attribute-Based Encryption (KP-ABE). The CP-ABE is does not support the updating the secret key without the decrypting the encrypted data file. In paper [13], the proposal of HABE extends to Key Policy Attribute-Based Encryption (KP-ABE), for user revocation and updating user's secret key updating is carried out by Proxy Re-Encryption (PRE) and Lazy Re-Encryption.

Paper [14] discusses Symmetric Encryption providing lightweight security solution to maintain data confidentiality on devices in a resource constrained scenario such as in a tactical network. However, lightweight encryption schemes are traditionally vulnerable to linear and differential cryptanalysis as well as power analysis attack when the encryption structure is known to the attacker. For tactical network devices, this is a critical concern since they often operate in hostile scenarios and lack in physical security in most cases. Moving Target Defense (MTD) is one of the key components of cyber maneuver that reshapes friendly networks and associated assets to be resilient to cyber-attacks. In this paper, we propose a lightweight reconfigurable symmetric encryption architecture, REA, which is capable of implementing a user defined symmetric encryption scheme as an MTD mechanism. The encryption structure can be customized from device to device based on their available resource and performance requirements. Due to the reconfigurable nature of the proposed architecture, it is not possible for an attacker to directly launch the cryptanalysis or power analysis attack before committing significant resources to retrieve the encryption structure first.

Digital content is easily spread out in the era of cloud computing. However, the challenge is providing an identity-based access control mechanism to carry out the rating system for preventing specific digital content from being obtained by inappropriate users. A novel identity based access control approach for digital content based on ciphertext-policy attribute-based encryption (iDAC) has been introduced in [15]. In iDAC, the access control still works even the digital content is duplicated to another content server. Moreover, only one copy of encrypted digital content is required to share with multiple users. This could efficiently reduce the overhead of content servers. As shown in our performance analysis with respect of security, space complexity, and time complexity, iDAC outperforms the traditional access control list based and encryption-based access control approaches.

PROPOSED METHODOLOGY

In this approach, the client has a collection of 'n' data's to outsource to the cloud server in the encrypted form. The encrypted data to be searchable by clients encrypt it using their own keys, and then outsource encrypted data to the server. To search over the entire document, collection of a given keyword is sent to the cloud server. After receiving the keyword, the server is responsible to search the index and return the corresponding set of encrypted documents.

ABE ALGORITHM DESCRIPTION

ABE techniques has been proven to offer better alternative as far as data encryption and decryption in cloud environment is concerned. This is due to the fact that certain attributes or features of the data is encrypted, unlike the conventional encryption/ decryption techniques and it has been proved to be more secure and robust. Another significant of this technique is that it has been extensively employed in critical real time systems. ABE can be classified into different categories, which can be shown in the fig 1 as follows.

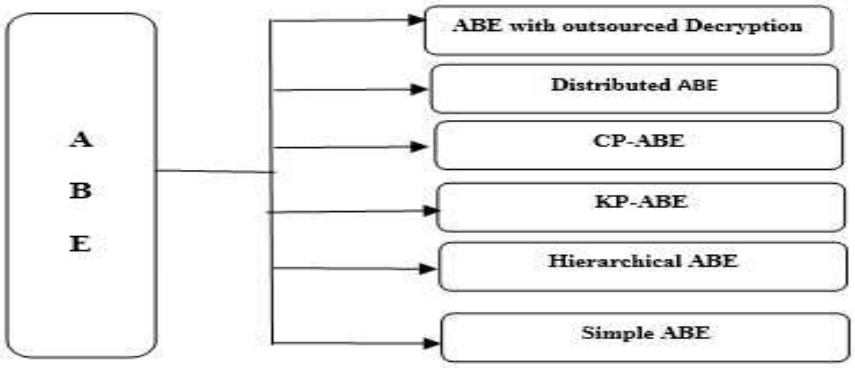

Figure 1: Classifications of ABE

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Here ABE comprising of cipher text (CP-ABE) is employed here. Proposed Algorithm has been developed in the following modules from A to Z along with the Keys as shown in the tabular representation as follows.

Table 1: Proposed encryption method for searching the encrypted data directly.

Key/Plain Text	1	2	3	4	5	6	7	8	9	0	+	-	*	/	=	^	.	I
Alphabetic Substitution	A	B	C	D	E	F	G	H	I	N	K	M	P	Q	L	R	W	Z

Encrypted data searching

In the encryption process, the client enters the numerical data with then corresponding private keys ('+',' –',' *',' /',' =',' ^', '.','i'). The private keys entered by client should compulsorily be an arithmetic operator. During the encryption process, the arithmetic operations are performed. The obtained result is then appended with the client data. Data and result values are then converted into floating point values. The resultant data is encrypted using the keyword table by searching the encrypted data directly. Each numeric value of the given example is mapped to the corresponding alphabets. (i.e. 1 mapped to A, + mapped to K etc.,)

To illustrate, Let the

Plaint text with private key: 128-50

Executed operation with result: 128-50=78

Floating point conversion: 128.0-50.0=78.0

Table 2: Conversion of Plain Text to Encrypted Text

Key/Plain Text	1	2	8	.	0	-	5	0	.	0	=	7	8	.	0
Encrypted Text	A	B	H	W	N	M	E	N	W	N	L	G	H	W	N

128,50 are the numerical value. '-' is the private key. The corresponding subtraction operation executed between 128 and 50. 128-50=78. The plain text "128-50" encrypted into "ABHWNMENWNLGHWN".

Flow Diagram for Encryption Process

The steps for encrypting searched data are illustrated in the flow chart (fig 2). The implementation of proposed encryption algorithm is essential for secure communication. It takes numeric data, plain text and key as parameters and can be straight forwardly adapted to various implementation contexts/security requirements. The pseudo code for encryption process is given in **APPENDIX-I**.

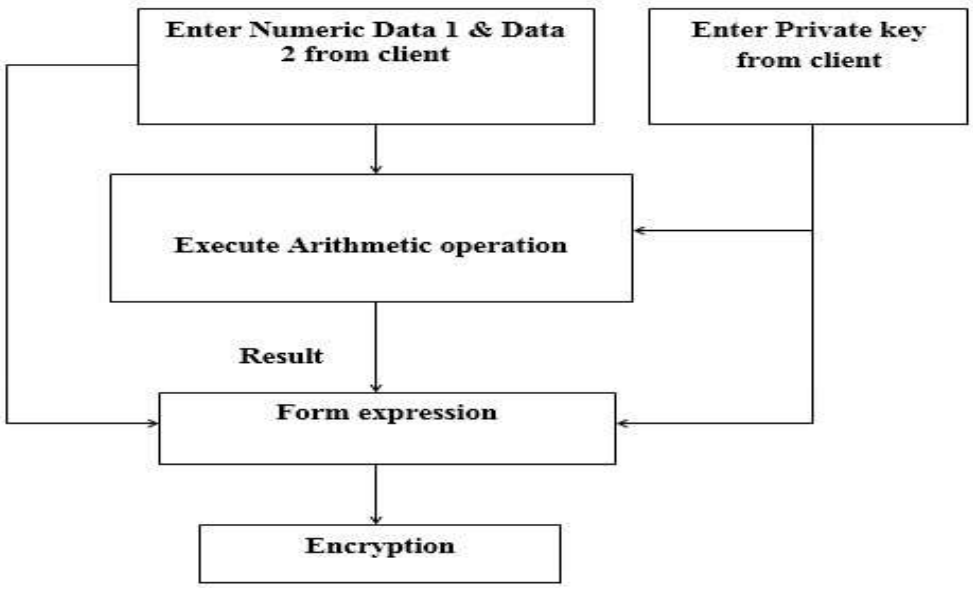

Figure 2: Encryption Flow Chart

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

SEARCH OPERATION

The attribute of encrypted data is stored in cloud server. If server searches a query, if the query attribute is compared with encrypted data attribute and match is found. The matched files are returned to the client.

PROPOSED METHOD ON SEARCHING QUERIES OVER INCOMPLETE DATA

The database attribute is stored in cloud server as an information system. A novel method of searching query over an incomplete data is proposed in this research. Search query process involving incomplete data (S) is done by extracting attributes from information system, which has attributes closely matching to S. There is a probability of attribute being missing from one of the databases. The client searches over the incomplete data and it is unable to find answers due to mismatch between query and information system attributes.

For an incomplete data, the information system does not contain the attribute value. Using proposed algorithm, answering query for unknown attribute is determined from the similar information system. Let S1 and S2 be two incomplete information systems having same set of attributes. Values of attributes (a_{S1} and a_{S2}) for both systems (S1 and S2) are similar. Using mapping, the relationship (z) between S1 and S2 can be calculated as a_{S2}- a_{S1}. S1 is transferred to S2 by this mapping technique which can
be represented as z (S1) =S2 or z (a_{S1}) =z (a_{S2}).

Table 3: Information system for Incomplete Data S1

X	**m**	**n**	**o**	**p**	**q**
x1	{(m_1,0.33), (m_2,0.66)}	{(n_1,0.66), (n_2,0.33)}	o_1	p_1	{(q_1,0.5), (q_2,0.5)}
x2	{(m_2,0.25), (m_3,0.75)}	n_1	{(o_1,0.33), (o_3,0.66)}	p_2	q_1
x3	m_1	n_2	{(o_1,0.5), (o_3,0.5)}	p_2	q_3
x4	m_3		o_2	p_1	{(q_1,0.66), (q_2,0.33)}
x5	{(m_1,0.66), (m_2,0.33)}	n_1	o_2	p_2	q_1
x6	m_2	n_2	o_3	p_2	{(q_2,0.33), (q_3,0.66)}

Table 4: Information system for Incomplete Data S2

X	**m**	**n**	**o**	**p**	**q**
x1	{(m_1,0.33), (m_2,0.66)}	{(n_1,0.66), (n_2,0.33)}	o_1	p_1	{(q_1,0.5), (q_2,0.5)}
x2	{(m_2,0.25), (m_3,0.75)}	{(n_1,0.33), (n_2,0.66)}		p_2	q_1
x3		n_2	{(o_1,0.5), (o_3,0.5)}	p_3	q_3

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

x4	m_3		o_2	p_1	{(q_1,0.66), (q_2,0.33)}
x5	{(m_1,0.66), (m_2,0.33)}	n_1	o_2		q_1
x6	m_2	n_2	o_3	p_2	{(q_2,0.33), (q_3,0.66)}

From table 3 and table 4 of S1 and S2 it is clear that unknown attribute values are determined by mapping technique which is subject to constraints that the original data is an integer. Attributed value of S2 is lesser than attributed value of S1. This is given by z (S1) =S2.

Decryption Technique
In decryption, encrypted data with their encrypted private key ('K', 'M',' P',' D',' L',' R', 'W','Z') is decrypted. The encrypted data is decrypted using the keyword table for numeric values of each letter, A mapped to 1, K mapped to +. Suppose we have

Encrypted data: ABHWNMENWNLGHWN
Delete W (floating point) and zero (0) from encrypted data: ABHMENLGH
Separate encrypted data into two sequences by L (equal): ABHM, ELGH,
First sequence consider as data: ABHMEN
Separate first sequence by encrypted private key of client: ABH, EN
Mapped data: 128, 50
The steps are represented in Table.5

Table 5. Representation of Decryption process.

Encrypted Text	A	B	H	W	N	M	E	N	W	N	L	G	H	W	N
Decrypted Text	1	2	8	.	0	-	5	0	.	0	=	7	8	.	0

128, 50 are the numerical value. '-' is the private key. The result of subtraction operation is 78. The decrypted plain text is "128-50". The pseudo code for Decryption process is given in **APPENDIX-II**.

Flow chart for decryption
Figure 3 shows the flow chart for decrypting the encrypted data using the keyword table.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

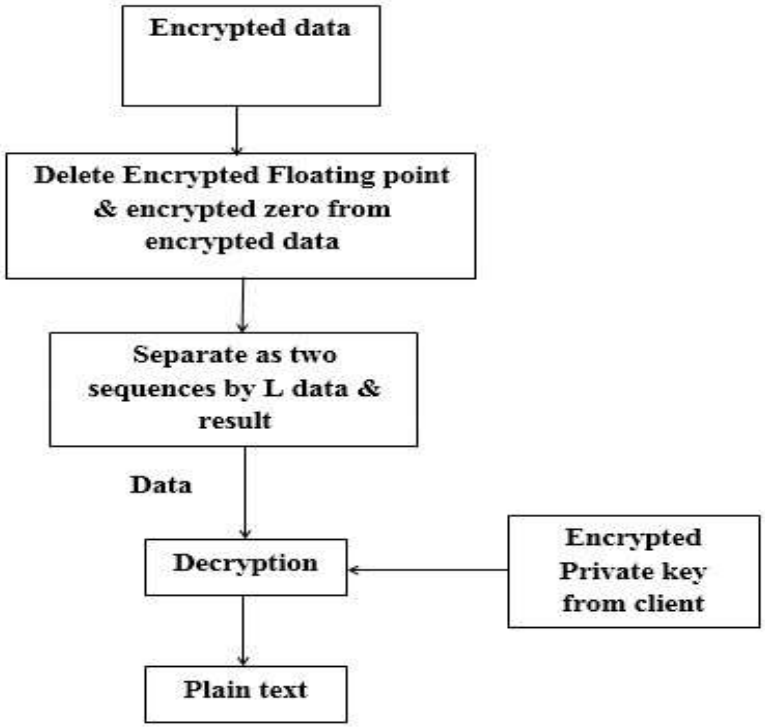

Figure 3: Flow chart of Decryption process

IMPLEMENTATION AND RESULTS

The encryption technique according to table 1 is implemented in J2EE platform and the output is shown in figure 3 for the sample input provided. The input includes numeric data, arithmetic expression (addition, subtraction, multiplication and division), power, exponentiation and also complex representation. The screen displays for the proposed encryption is shown in Figure 4.

Output Screen Display
Input data
162 + 138
128-50
28 * 2
11 ^ 2

Encrypted Data

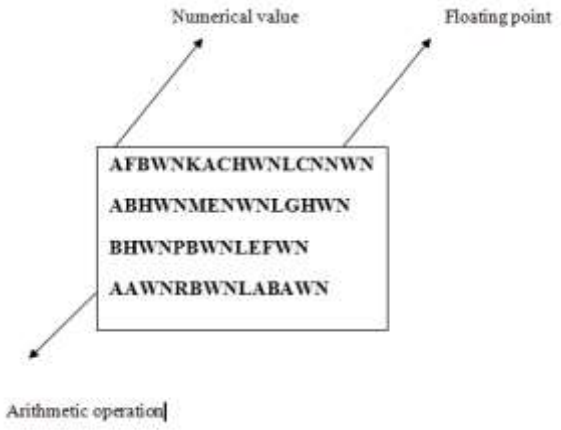

Figure 4: Encrypted Output

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

In table 5 and table 6, the computational speed of encryption and decryption and the complexity analysis of the reported and proposed algorithm has been mentioned.

Table 5: Computational Speed of Encryption and Decryption

Speed of Encryption/Decryption in sec	**Size of Data in MB**	
	Proposed	**Reported**
10	1000	850
20	2000	1700
30	3000	2550
40	4000	3400
50	5000	4250

Table 6: Comparative analysis of Complexities of Proposed and Reported approach

Complexity in Time Period in sec	**Size of Data in MB**	
	Proposed	**Reported**
0.2	350	500
0.4	700	1000
0.6	1050	1500
0.8	1400	2000
1.0	1750	2500
1.2	2100	3000
1.4	2450	3500
1.6	2800	4000

In figure 5 and figure 6, the search time and retrieval time of the documents using the proposed and reported approach is compared and one can infer from the above result clearly that the proposed algorithm is efficient when compared to the more traditional approach.

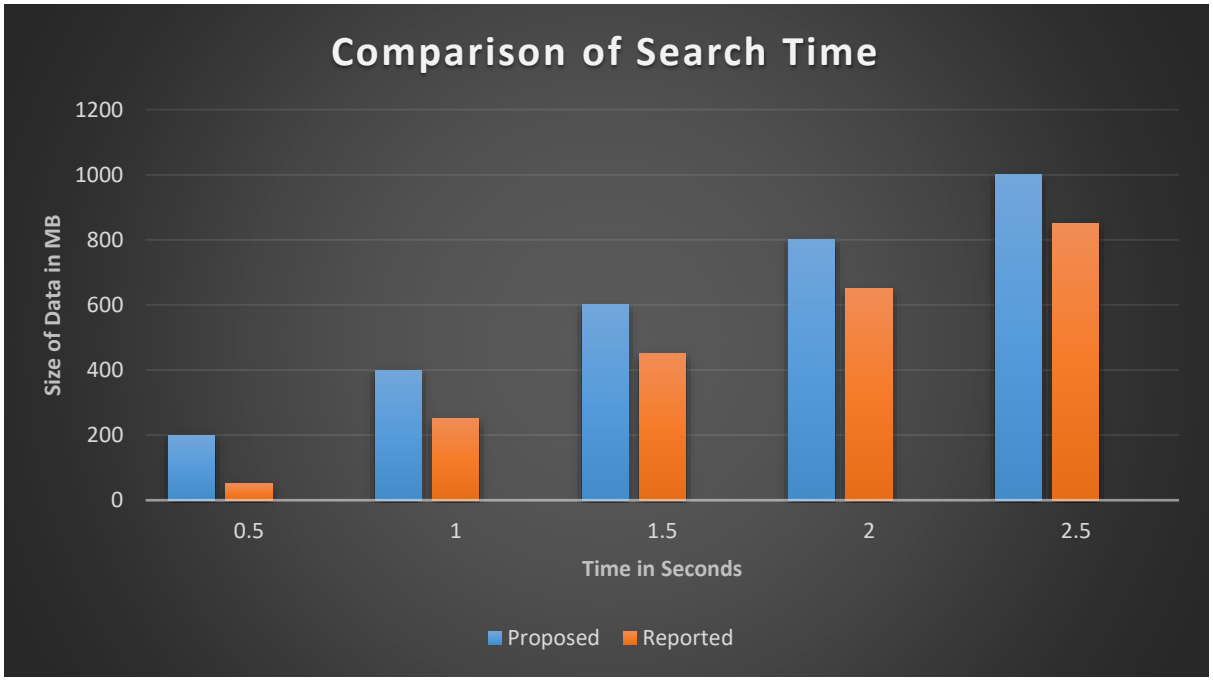

Figure 5: Comparison of Search time

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

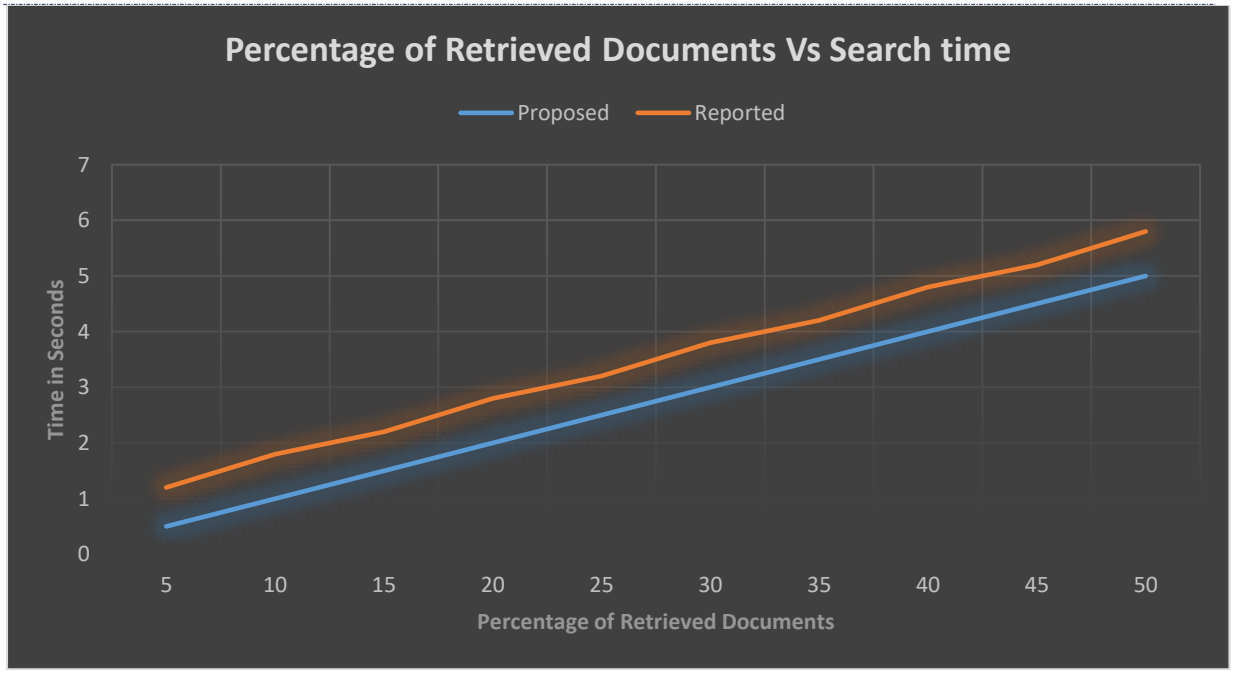

Figure 6: Comparison of Retrieved documents

CONCLUSION

In this work the Attribute Based Encryption (ABE) technique is proposed and it is achieved by encrypting and decrypting the input data by means of client's private key. The significance of this technique lies in the query searching based on the attribute of the data. Query search over the incomplete data is achieved by extracting missing attributes from comparable relative files. The encryption programming is implemented in java threads. By this algorithm, client securely outsources its data on cloud server and searching encrypted data and decrypting becomes relatively easy by applying our proposed algorithm and its efficiency has been proved. This research being a software simulation, the system's processor plays a key role in encryption and many cloud providers will only offer basic encryption on a few database fields, such as passwords and account numbers, and with the sudden increase in data size, the encryption process slows down considerably. Therefore the solution lies as a future scope in the hardware implementation of this algorithm that can be done to enhance the computational speed along with the enhanced security features.

REFERENCES

[1] Saravana Kumar N,Rajya Lakshmi G.V and Balamurugan B "Enhanced Attribute Based Encryption for Cloud Computing", *ELSEVIER International Conference on Information and Communication Technologies*, vol.46, pp.689-696, 2015.

[2] Hao Wang , Bo Yang and Yilei Wang "Server Aided Ciphertext-Policy Attribute-Based Encryption", *IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*, pp.440-444,2015.

[3] Srinivasan Nagaraj, Dr.G.S.V.P.Raju and V.Srinadth "Data Encryption and Authetication Using Public Key Approach", *ELSEVIER International Conference on Intelligent Computing, Communication & Convergence*, vol.48, pp. 126-132, 2015.

[4] Prakash G L, Dr. Manish Prateek and Dr. Inder Singh "Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System", *IEEE International Conference on Signal Propagation and Computer Technology*, pp.624-629, 2014.

[5] A. N. Borodzhieva and P. K. Manoilov "Training Module with Graphical User Interface for Encryption and Decryption Using Affine Ciphers Applied in Cryptosystems", *IEEE 20th International Symposium for Design and Technology in Electronic Packaging*, pp.281-286.

[6] Mohamed Ali, Hamza Ali, Ting Zhong, Fagen Li, Zhiguan Qin and Ahmed Abdelrahaman A. A "Broadcast Searchable Keyword Encryption", *IEEE 17th International Conference on Computational Science and Engineering*, pp.1010-1016, 2014.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

[7] Jianting Ning, Xiaolei Dong, Zhenfu Cao and Xiaodong Lin "White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes", *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp.1274-1288, 2015.
[8] Nikita Gorasiaa, R.R.Srikanth, Dr. Nishant Doshi and Jay Rupareliya "Improving Security in Multi Authority Attribute Based Encryption with Fast Decryption", *ELSEVIER 7th International Conference on Communication, Computing and Virtualization*, vol.79, pp.632-639, 2016.
[9] Baodong Qin, Robert H. Deng, Shengli Liu, and Siqi Ma "Attribute-Based Encryption with Efficient Verifiable Outsourced Decryption", *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 7, pp. 1384-1393, 2015
[10] Yun Wang, Dalei Zhang and Hong Zhong "Multi-authority Based Weighted Attribute Encryption Scheme in Cloud Computing", *IEEE 10th International Conference on Natural Computation*, pp.1033-1038, 2014.
[11] Anuradha Meharwade and G. A. Patil "Efficient Keyword Search over Encrypted Cloud Data", *ELSEVIER First International Conference on Information Security & Privacy*, vol.78,pp.139-145,2016.
[12] Peng Xu, Tengfei Jiao, Qianhong Wu, Wei Wang and Hai Jin "Conditional Identity-Based Broadcast Proxy Re-Encryption and Its Application to Cloud Email", *IEEE Transactions on Computers*, vol. 65, no. 1, pp.66-79, 2016
[13] P.Praveen Chandar, D. Muthuraman and M.Rathinraj "Hierarchical Attribute Based Proxy Re-Encryption Access Control in Cloud Computing", *IEEE International Conference on Circuit, Power and Computing Technologies*, pp.1565-1570, 2014.
[14] Mohammad Iftekhar Husain, Kerry Courtright and Ramalingam Sridhar "Lightweight Reconfigurable Encryption Architecture for Moving Target Defense", *IEEE Military Communications Conference*, pp.214-219, 2013.
[15] Win-Bin Huang and Wei-Tsung Su "Identity-based Access Control for Digital Content based on Ciphertext-Policy Attribute-Based Encryption", *IEEE International Conference on Information Networking*, pp.87-91,2015.

APPENDIX –I
Pseudo code for Encryption Operation
set index i=0 for formed expression
for(length of formed expression)
switch (expression(i))
case (i)
expression(i)==numeric data
expression (i)=(A or B or C or D or E or F or G or H or I)
case (ii)
expression(i)==arithmetic operator
expression(i)=(K or M or Q or P)
case (iii)
expression(i)==Power
expression(i)=R
case (iv)
expression(i)==floating point
expression(i)=W
end switch statement
end for statement return expression

APPENDIX-II
Pseudo code for Decryption Operation
set index i=0 for encrypted data sequences
for length of encrypted data sequences
switch(expression(i))
case (i)
expression(i)== (A or B or C or D or E or F or G or H or I)
expression (i)= (0 to 9)
case (ii)
expression(i)== (K or M or Q or P)

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

expression(i)= arithmetic operator
case (iii)
expression(i)==R
expression(i)=Power
case (iv)
expression(i)==W
expression(i)= floating point
end switch statement
end for statement
return plain text