Volume 4, Issue 12, December 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Novel Trust Dependent Attribute Based Encryption (TD-ABE) for Improving the Cloud Security

[1]Vinod Kumar Pandey, [2]Sandeep Kumar Patel (Sandy), [3]Swati Bedre

[1, 2] Subharti Institute of Technolog & Engineering, Swami Vivekanand University Meerut (U.P.), India

[3] Technocrats Institute of Technology (Excellence), Rajiv Gandhi Proudyogiki Vishwavidyalay, Bhopal (M.P.), India

Abstract: ***Data is a valuable asset which always cost more than the infrastructure provided to make its transaction secure and fast. Applications of today's world are totally dependent on data and their effective exchanges by which some logics or decisions can be derived for forecasting the affects. For providing the above requirements a new computing paradigm has evolved termed as cloud computing. It is the combination of different computing phenomenon's such as distributed, grid, autonomic, scalable and fault tolerant. Along with the size of data the users demands with respect to security is gets increased making the new area of work for researchers because of its heterogeneous environment. Traditionally security can be treated as a process of applying cryptography and authentication by which clients data is secured from the storage or service provider. But with cloud computing all the services can be delivered by web based system in which the data needs to be passed to the application server for performing any types of operation. So in such situation the data is not secure from the client machine to the application server. In this end no security algorithm can be applied. Also the security algorithms dependencies are totally in hand of provider which might cause data losses in future or can lose in privacy and confidentiality. Thus some controls needs to be given to the user for increasing the trust over the system. Thus this work proposes novel trust dependent attribute based encryption using user based key policies for improving the cloud security. At the analytical level of evaluation the approach is showing its strong presence among its competitors.***

Index Terms- Cloud Computing, KP-ABE (Key Policy-Attribute Based Encryption), TD-ABE (Trust Dependent Attribute Based Encryption), Access Policy;

I. INTRODUCTION

Information is profitable holdings for customer considering particular, business, social and wellbeing data frequently sharable separate to time and prerequisite. The absence of transforming time and capacity limit or spare assets cost information put away at third place known as cloud suppliers rather than customer utilize its assets. On the other hand, there have been wide protection concerns as information

could be presented to those third place servers and to unapproved gatherings. To guarantee the customer control over access to its information's, it is a swearing up and down to method to make information garbled and non-interpretable structure [1]. To make information in garbled structure uncountable methodologies are exhorted via scrutinizes. Fundamentally the system to make information mixed up structure is named as encryption or cryptography. Cryptography or encryption calculations act a paramount part in information security.

Information stockpiling on cloud is given by the administration supplier. Capacity of this information on un-trusted capacity makes secure information offering a testing issue. Secrecy of the information on this obscure environment might be accomplished by means of different access control & encryption system. Expected encryption measures & procedures will just give the fundamental things of security which could be ruptured. To attain fine grained access control & powerful information access control strategies property based encryption is overall characterized standard [2]. There are different encryption calculations accessible like AES, 3des, blowfish and so forth which will likewise give the encryption based security however in a characterized way [3]. It is an oppressive of client to manage their complex procedures. For further changes in existing procedure of security this work concentrates on characteristic based encryption with trust esteem. This work depict the essential utility of applying quality based encryption (ABE) for information offering on un trusted capacity & servers.

As indicated by the pointed out issue the space cloud security this work gives the answer for the specified security issues through TD-ABE convention stack in two steps. In first step, the client concentrates on the repudiation strategies focused around ABE. It gives the right to gain entrance control system as indicated by the client access verifiable subtle elements. The proposed plan of TD-ABE shrouds the client's information own arrangement from itself & the server. In second step the plan propose the ABE based one of a kind key era for encryption & decoding for distributed storage. This key could be produced without the information of getting to profile client & is carried out by selecting the irregular traits from client table.

As cloud requisitions is picking up prevalence nowadays so as their provisions additionally, as in medicinal services, military, transportation, business sagacity, managing an account, and in data advances requisitions. IT is the part which is influenced at most by these fresher innovations and is demonstrating enchantment apparatuses before its clients. These

change n situations has came in light of ABE's relevance over the different territories. Some of those properties is displayed here as takes after:

(i) ***Flexibility:*** ABE composes client properties into a recursive set structure and permits clients to force dynamic imperatives on how those ascribes may be consolidated to fulfill a strategy. So ABE can help compound properties and different numerical assignments for a given quality advantageously.

(ii) ***Fine-grained access control****:* Based on ABE plan can undoubtedly attain fine-grained access control. An information manager can characterize and implement expressive and adaptable access arrangement for information records as the plan.

(iii) ***User Revocation****:* To manage client renouncement in distributed computing, ABE adds a credit to each client's key and utilize various worth assignments for this property. So we can redesign client's key by essentially increasing the value of the current key. The methodology simply oblige an area power to keep up some state data of the client keys and maintain a strategic distance from the need to create and disperse new keys on an incessant premise, which makes our plan more productive than existing plans.

(iv)***Expressive Ability****:* In ABE, a client's key is connected with a situated of qualities, so ABE is reasonably closer to customary access control strategies, for example, Role-Based Access Control (RBAC). Consequently, it is more regular to apply ABE, rather than KP-ABE, to uphold access control.

II. BACKGROUND

Users that use cloud services will typically pay only for the amount of storage it uses and computation it performs and the network infrastructure in uses but it doesn't pay for the maintenance purpose. In additional to that it provides the secure storage capacity and data backups & recovery. But these data is stored at third party locations thus needs more trust on the cloud providers. A major concern that is typically not sufficiently addressed in practice which is [5]:

"The data stored at cloud locations may be accessed and read by a cloud administrator without knowledge of the client. A cloud administrator may not be trusted despite the presence of contractual security obligations, if data security is not further enforced through technical means. "

Therefore, it is useful to apply software techniques, such as encryption keys, to ensure that the confidentiality of cloud data is preserved at all times. It is especially crucial to safeguard sensitive user data such as e-mails, personal customer information, financial records, and medical records. However, the main purpose of the access control based cryptography is not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation for cloud based data records [6, 7]. Anonymous access control is a very desirable property in various applications, e.g. encrypted storage in distributed environments; and attribute based encryption is a cryptographic scheme that is targeted to achieve this property. ABE is an encryption mechanism that is useful in settings where the list of users may not be known prior. Here, all users may possess some credentials, and these are used to determine access control and also provide a reasonable degree of anonymity with respect to the user's identity. Due to these shortcomings of traditional access control mechanisms, cryptographically enforced access control receives increasing attention.

To deal with the above mentioned objectives of access control & better encryption standard one of the most promising approach can be used named as attribute based encryption through cipher text only policies. In this scheme, users possess sets of attributes (and corresponding secret attribute keys) that describe certain properties. Ciphertexts are encrypted according to an access control policy, formulated as a Boolean formula over the attributes. The construction assures that only users whose attributes satisfy the access control policy are able to decrypt the ciphertexts with their secret attribute keys [8]. The construction is required to satisfy a collusion resistance property: It must be impossible for several users to pool their attribute keys such that they are able to decrypt a ciphertexts which they would not be able to decrypt individually. There are so many other transformation based schemes available like HNT Transformation [9], Bayes Network & HMM [10] & hop by hop mechanism for authentication [11]. These above security & authentication mechanism can also be applied in various other domains like used in [12].

Ciphertexts policy attribute based encryption is a scheme that gives a natural way to separate the credentials from the access policy and cleverly combine them at a later stage to provide secure access to protected data. In most ABE schemes the size of the ciphertexts is quite large and is of the order of the number of attributes. In this work we present our approach for a multi-level threshold attribute based encryption which is independent of the number of attributes. There are two major features to attribute based encryption:

- It has the capacity to address complex access control policies.
- The exact list of users need not be known apriori. Knowledge of the access policy is sufficient.

Also, an important property that attributes based encryption schemes must satisfy is that of collusion resistance. Collusion resistance means that, if 2 or more users possessing different keys combine to decrypt the ciphertexts, they will be successful if and only if any one of the users could have decrypted it individually. In other words, even if multiple parties collude, they should not be able to decrypt the ciphertexts unless one of them was able to decrypt it completely by herself. These properties ensure that only users possessing the right keys have access to the information. Moreover, as the encryption is based on the access-structure it implicitly assures anonymous access control.

Some more extension is proposed in [12] like SIP model for mutual authentication of different cloud user & risk-aware approach which is based on an extended Dempster-Shafer mathematical theory of evidence. While studying about the existing approaches the various researchers is found to be focused on two main things; access control & encryption

standards. As like in [13] a new distributed environment attribute based encryption is proposed which is based on Ciphertext-Policy. It is known as CP-ABE and where policies are associated with encrypted data and attributes are associated with keys. In this work we focus on improving the flexibility of representing user attributes in keys.

Further extension to that Ciphertext Policy Attribute Set Based Encryption (CP-ASBE) is proposed - which, unlike existing CP-ABE schemes that represent user attributes as a monolithic set in keys, organizes user attributes into a recursive set based structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. Similarly so many approach is been proposed by researcher during the last few years to deals with such fine grained access control mechanism using ABE. Likewise given extended RBAC [14], TAAC [15], TABE [16] and DAAC [17]. Some of the authors had also focused their work on policy settings through access identification like in [18]. In this the author categorizes the security according to its requirements of revocable storage & giving protection to newly encrypted data.

III. PROBLEM STATEMENT

In storing the data at third place client not sure about the information stored safely. There possibility of different attacks during the storage and retrieval of data to/from third location. Data may be tampered and accessed by unauthorized user or external attacker. To make safety and maintain privacy its needs number of security mechanisms. Thus by verifying the formulation of problem we can get the better results in case of both the types of attribute based encryption KP-ABE [19] & CP-ABE [20]. We need to keep in concern about the various objectives of data security on this un-trusted server of cloud & storage as given. The above scenario shows an identified problem that realized at client end during the retrieval and storing of information at cloud. Here might be any attacker or unauthorized person or attacker present to tamper or access the data before data reach at client or cloud providers. Attacker may be influence client personal or financial life so here need to prevent from this kind of activity need lot of techniques are used to during data storage. To solve this problem one approach is also proposed by our-self to keep data safe from unauthorized access. We consider the server to be semi-trusted, i.e., honest but curious. That means the server will try to find out as much secret information in the stored record files as possible, but they will honestly follow the protocol in general. On the other hand, some users will also try to access the files beyond their privileges. To do so, they may collude with other users, or even with the server. In addition, we assume each party in our system is preloaded with a public/private key pair, and entity authentication can be done by traditional challenge-response protocols. After analysing the various researchers work about cloud security [22], distributed security [23], HASBE [21] framework & client end cloud services [24] the TBSSM can categorizes this requirements according to their use.

Thus to apply the ABE correctly one needs to deal with all the dynamic attributes and update the same as desired. After studying the different approaches that can be applied to deal with the dynamic attributes this work can formulate the following are the minimum requirements of any dynamic attribute-updating scheme:

1. One must be able to add/delete/update any dynamic attribute, in any number and at any desired instance.
2. One must be able to assign any desired value to a chosen dynamic attribute.
3. The modification of one attribute value must be independent of the same to the other.

IV. PROPOSED TD-ABE APPROACH

Web and systems requisitions are developing quickly. So the criticalness and the estimation of the traded information over the web are expanding. Data Security has been extremely paramount issue in information correspondence. Any misfortune or risk to data can turn out to be extraordinary misfortune to the association. Encryption system assumes a fundamental part in data security frameworks. Among the entire encryption systems trait based encryption (ABE) is getting prevalence step by step. For secure information get to the customer must make certain about the methodology utilized for this kind of encryption yet in cloud stage everything is given by cloud. Along these lines the fulfilment of security at client level is not given by any cloud. Hence this work proposes a novel Client end trust ward characteristic based encryption (TD-ABE) for attaining the better comes about. This work concentrates on the requisition region of distributed storage stage for client fulfilment.

This model gives an extraordinary stack based answer for accomplishing the end client security. As indicated by ABE the client might have the capacity to decode the record on the premise of the document quality, which is diverse for each one document & relies on upon the client class. In this philosophy the quality might be distinguished from the client characteristic table. This trait table is dynamic in nature & whose qualities are passed in the table after a pre-calculation of trust & client demonstrating. At starting level our proposed methodology appears to be better secure information get to in correlation to other existing system.

Architectural Description

Unapproved access of information, cloud made questionable for customer. To give unwavering quality on cloud, a methodology TD-ABE is exhorted at customer end to make sheltered and secure capacity of information. The proposed methodology is stack of various assurances layer that arrangements with customers' information to giving covering layers of verification conduct investigation and make information disjointed structure utilizing conduct based encryption systems. The proposed TD-ABE methodology comprises of a few stages. Firstly to covered verification layer to the information by giving character of clients and checking the asserted personality. Besides to covered conduct investigation layer to the information by consistent watching the exercises of clients on the premise of verifiable property. Third stage

is to covered conduct based encryption layer by changing over customer information into scrambled information and send for capacity on the cloud. Figure 1 delineated proposed methodology.

The proposed TD-ABE model shows stack of security layer for the customer information that are covered in distinctive of stages, for example, Authentication basically secures personality, not what that character is approved to do or what access benefits he or she has; this is a different choice related strictly to commission. The partition of these three capacities (Registration, Authentication and Authorization) by entrusting them to particular substances might be useful from a security improving point of view, as it connections and confines the reasonable information handling movements and the accessibility of individual information to the particular errands of every on-screen character.

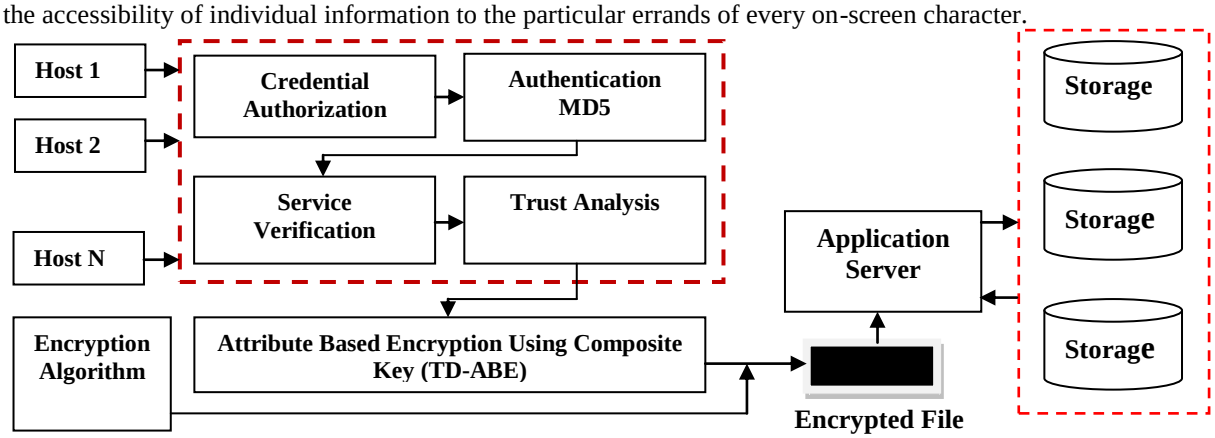


Figure 1:- Proposed TD-ABE Security Using ABE

Methodology: Stack Based Approach

Stack methodology took after to propose result of issue. Distinctive layers of stack convention covered on the customer information one by one to make secure and safe information. It likewise secures information from unapproved access. It first stage is verification in which the kind of client access & record needed is attained at provision server by utilizing the hash digest estimation utilizing Md5. Next is sanction in which the client class & its trait are approved from a client database. Presently the administration gave by the cloud again need to confirm utilizing portlet administration check. Essentially the trust is figured worth which is more that a particular edge which is characterized by the client arrangements. It gives a knowledge to client exercises which is characterized after its trust check. The aforementioned trust of each client is examined by its recorded information access & sort of documents needed. It is focused around client classification and access control approaches. It is the last procedure of TD-ABE in which a particular ABE encryption technique is utilized to scramble & decode the record for client access. It is focused around above trust & conduct investigation. In this every encryption is carried out by passing the estimation of client property as a key. In this the span of key is focused around number of characteristic utilized.

TD-ABE Stack

(i) **Authentication: -** In this the sort of client access & document needed is attained through a verification stage at requisition server.

(ii) **Authorization:** - The client class & its trait are commissioned from a client database.
Portlet Service confirmation: - In this step the administration gave by cloud is confirmed in program & gives a distinguishing proof estimation of honesty.

(iii) **Trust Calculation:** - In this step every client need to achieve an interesting trust esteem which is more that a particular limit which is characterized by the client arrangements.
It gives a knowledge to client exercises which is characterized after its trust confirmation.

(iv) **User Attribute Based Encryption:** - It is the last methodology of TD-ABE in which a particular ABE encryption approach is utilized to encode & unscramble the document for client access. It is focused around above trust & conduct investigation. In this every encryption is carried out by passing the estimation of client characteristic as a key. In this the extent of key is focused around number of characteristic.

Expected Outcomes

Cutting edge after-effects of the strategy may demonstrate the change in giving the customer level security through nature's turf. It gives the high end unwavering quality towards the new introduction of the framework. The outsider system manages conduct based encryption in which different administrations is given like portlet confirmation, key era, trust ID. Out of these strategies an upgraded secure situations is produced through our proposed TD-ABE. At the introductory level of our exploration we get the accompanying profits.

- It holds dependability on outsider area
- Client guarantees about information stockpiling in protected way and unapproved access.
- It secure information from distinctive strike at customer end.
- It may be got creative methodology at customer end in cloud stage for distinctive provision spaces.
- The capacity & calculation expense might be minimized.

- The trait encryption gives a wide go for key era through characteristic.
- In this the validation is accomplished.

Application Areas

Now days the trust based mechanism is applicable for various online data storing applications including the web based and mobile based version. Some of the application where the suggested scheme can be effectively used for improved security and control over data and its modifications are:

(i) Social networking
(ii) Messaging services
(iii) Mailing service
(iv) Online document sharing
(v) Record Based Systems
(vi) Enterprise Resource Planning
(vii) Business intelligence
(viii) Transportation systems

V. RESULT EVALUATIONS

The suggested TD-ABE approach proves its importance at various stages of data security and gives more proves to the low end users. The results are evaluated on various parameters of data confidentiality, availability and integrity. Apart from that there are different factors which are also capable of measuring the efficiency of such mechanism. These are security analysis, fine grained access control, user's access privilege security etc. Result is categorized in various tables is given as below:

Table 1

S. No	UserID / Password	Credential Size: User ID Size (Bit)	Credential Size: Pass-word Size	Digest Generated	Hash Size (Bits)	Meth-od Used
1	Sandeep123 / 123456789	224	144	25f9e794323b453885f5181f1b624d0b	128	MD5
2	Sandy2013 / attribute2013	608	352	4c16c148d0c9a3147cda479945e899c3	128	MD5
3	swati123 / bahgwan2020	416	256	148d0c925f9e794323b5f5181f1b1b62	128	MD5

Table-II: Key Value Attributes Combinations

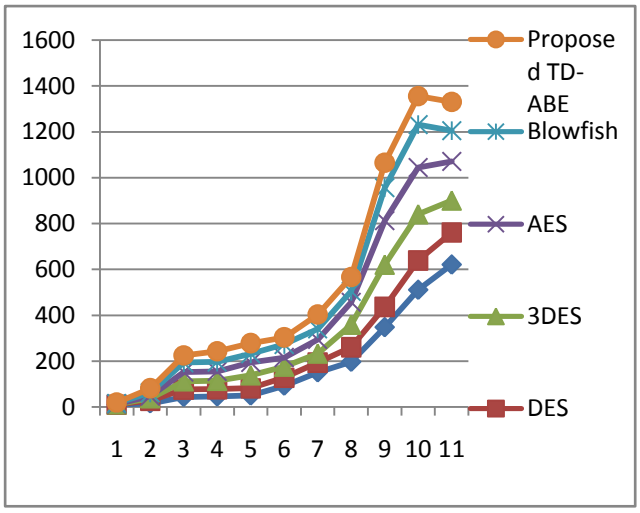
S. No	Key Name	Key Elements
1	K1	UserID, Password, Timestamp
2	K2	Login Failed Attempts (LFA)
3	K3	Type of File Access (TFA)
4	K4	Total Number of Services
5	K5	Composite Key Generated

Table-III: Comparison of TD-ABE with Existing Encryption Standards for Various Inputs

Algorithm	Encryption Time (MiliSec)											Throughput = Age Size / Time
Size(Kb)	**10**	**16**	**44**	**46**	**50**	**93**	**151**	**197**	**348**	**511**	**621**	
DES	1	12	32	32	32	35	43	64	89	128	140	3.08
3DES	0	10	36	36	56	48	39	98	184	202	140	3.46
AES	2	10	41	41	56	40	62	98	192	204	170	3.28
Blowfish	3	14	41	41	38	57	46	48	144	187	135	2.75
Proposed TD-ABE	4	20	31	47	47	31	63	62	109	124	125	3.16

Table-II & Table-III: It is again a description and generation of multiple keys which is taken out from users behavioural Elements. This behavioural attributes are different for different users & thus ABE is using this values as a unique key for providing the data confidentiality and isolation. It can be a combination of multiple elements likewise in k1 which is

combination of userid, password and current timestamp. Similarly K2 to k4 is created. Now in k5 the work had XoRed all the above keys to generate a composite key with same size but the kind of security provided by that is very high.



Graph 1: The above graph shows the throughput measurement, encryption and key generation time measurement and proves that the suggested approach of TD-ABE based ABE is efficient than other existing approaches. It takes the files of various types of formats and size even though its encryption and key generation time is minimum than others. Thus it provides the high end reliability towards the new orientation of the system. The third party mechanism deals with behaviour based encryption in which multiple services is given like portlet verification, key generation, trust identification. Out of these methods an enhanced secure scenarios is generated through our proposed TD-ABE.

VI. CONCLUSION

This work gives a trust dependent attribute based encryption TD-ABE to expand the security & dependability of the end client to any of the cloud administration or customer server construction modelling. In this when client saves its information at outsider area than there must be some security results accessible with those to make the information secure and expands the clients trust & dependability over capacity supplier. Another client dependably tries to conquer the dependability components for the information misfortune. This private data will need to be secure & access must be far from security ruptures. The TD-ABE utilizes an extraordinary stack based methodology model which gives security additional items to the current systems. The proposed model utilization client characteristic components and the sorts of information which it was utilizing as a key component for creating the key. Lastly a composite key is produced which is passed for encryption. Hence the component is equipped for giving the information separation and access benefits for distinctive clients and gives the information categorization as per their profile components. Besides, proposed plan can empower the information holder to delegate a large portion of calculation overhead to effective cloud servers. Classified process of client access benefit and client mystery key responsibility could be attained. Result assessment demonstrates the proficiency of proposed approach and appears to be better secure information get to in correlation to other existing procedure.

VII. FUTURE WORK

Some of the goals of the proposed algorithms that will achieve in the future are:

1. *Optimal Resource Utilization:*-Minimize the number and size of the data structures required to implement the algorithms,
2. *Time Efficient:*-Trust calculation based on an input parameter must be fast & accurate. Key generation can also be synchronized with ABE.
3. *Service Verification:*-Allow every user to verify the service which it was getting for customer satisfaction,
4. *Policy Updation:*-Maximize the stability in the cloud through higher security. It can be done by giving the facility of dynamic policy updation to the end user.

REFERENCES

[1] Ming Li, Shucheng Yu, Yao Zheng, Student, Kui Ren, & Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption" in IEEE Transactions on Parallel & Distributed systems, 2012.

[2] Pratap Chandra Mandal, "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish" in JGRCS, Volume 3, No. 8, August 2012.

[3] Deepak Garg, Limin Jia & Anupam Datta " Policy Auditing over Incomplete Logs: Theory, Implementation and Applications" in ACM 978-1-4503-0948-6/11/10 in 2011.

[4] Yanlin Li, Jonathan M. McCune, and Adrian Perrig, "VIPER: Verifying the Integrity of PERipherals' Firmware" in ACM 978-1-4503-0948-6/11/10 in 2011.

[5] Eric Y. Chen, Jason Bau & Charles Reis "App Isolation: Get the Security of Multiple Browsers with Just One" in ACM 978-1-4503-0948-6/11/10 in 2011.

[6] Jiyong Jang , David Brumley & Shobha Venkataraman in " BitShred: Feature Hashing Malware for Scalable Triage and Semantic Analysis" in ACM 978-1-4503-0948-6/11/10 in 2011.

[7] Vishwa gupta,. Gajendra Singh & Ravindra Gupta, "Advance cryptography algorithm for improving data security " in IJARCSSE Volume 2, Issue 1ISSN: 2277 128X , Jan 2012.

[8] Omar Elkeelan & Adegoke Olabisi, "Performance Comparisons, Design, and Implementation of RC5 Symmetric Encryption Core using Reconfigurable Hardware" in Acedmic Publisher, 2008.

[9] Sasirekha N, Hemalatha M , "An Enhanced Code Encryption Approach with HNT Transformations for Software Security", International Journal of Computer Applications (0975 – 8887) Volume 53– No.10, September 2012

[10] Nagaraju Devarakonda, Srinivasulu Pamidi, V Valli Kumari & A Govardhan, " Integrated Bayes Network and Hidden Markov Model for Host Based IDS" in IJCA Volume 41– No.20, March 2012.

[11] Maisam Mohammadian, Nasser Mozayani, "Improving of Authentication Mechanism in IMS Environment By Integration Hop By Hop And End To End Model", International Journal of Soft Computing And Software Engineering (JSCSE) e-ISSN: 2251-7545 Vol.2, 2012 .

[12] Ziming Zhao & Gail-Joon Ahn, "Risk-Aware Mitigation for MANET Routing Attacks" in IEEE Transaction on dependable & secure computing, vol 9, no 2, 2012.

[13] Rakesh Bobba, Himanshu Khurana & Manoj Prabhakaran, "Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption" in University of Illinois at Urbana-Champaign, July 2009.

[14] John Bethencourt, Amit Sahai & Brent Waters, "Ciphertext-Policy Attribute-Based Encryption", in NSF CNS-0524252 US Army Research, in 2009.

[15] Kan Yang, Zhen Liu, Zhenfu Cao, Xiaohua Jia, Duncan S. Wong & Kui Ren, "TAAC: Temporal Attribute-based Access Control for Multi-Authority Cloud Storage Systems" in University at Buffalo, 2011.

[16] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Xiaorui Gong & Shimin Chen, "POSTER: Temporal Attribute-Based Encryption in Clouds" in ACM CCS 11, ISSN: 978-1-4503-0948-6/11/10, Dec 2011.

[17] Sushmita Ruj, Amiya Nayak & Ivan Stojmenovic, "DACC: Distributed Access Control in Clouds" in IEEE TrustCom-11/IEEE ICESS-11, ISSN 978-0-7695-4600-1/11, 2011.

[18] Amit Sahai & Hakan Seyalioglu, "Dynamic Credentials and Ciphertext Delegation for Attribute-Based Encryption" in DARPA N11AP20006, University of Texas, Aug 2012.

[19] Changji Wang & Jianfa Luo, "An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length" in Mathematical Problems in Engineering Volume 19 , Article ID 810969, 2013.

[20] Nishant Doshi & Devesh Jinwala, "Updating Attribute in CP-ABE: A New Approach" in IJCA ICDCIT , ISSN 0975 – 8887, 2013.

[21] Neena Antony & A. Alfred Raja Melvin, "An Efficient Approach For Flexible And Scalable Access Control Through HASBE" in IJCSMR Vol 2 Issue 4, ISSN 2278-733X, April 2013.

[22] Sunitha Muppa, R. Lakshman Naik & Chalapathi Valupula, "Secure Scheme of Data Protection in Cloud Computing" in IJCST Vol. 3, Issue 1, ISSN : 0976-8491, Mar 2012.

[23] Shilpa Elsa Abraham, "Distributed Attribute Based Encryption for Patient Health Record Security under Clouds" in IJCTT, Vol 4 Issue 3, 2013.

[24] Anup R. Nimje, V. T. Gaikwad & H. N. Datir, "Attribute-Based Encryption Techniques in Cloud Computing Security : An Overview" in IJCTT, Vol 4 Issue 3, 2013.

