Trust based Security Service Mechanism for Client End Security using Attribute based Encryption at Cloud Platform

Balwant Prajapat
Department of Computer Science & Engineering
Patel Institute of Technology, Bhopal (M.P), India

Surendra Vishwakarma
Department of Computer Science & Engineering
Patel Institute of Technology, Bhopal (M.P), India

ABSTRACT
Internet and cloud application is getting faster day by day. It increases the data exchange rate over internet. During this heavy data transmission security is considered as major issues in communication. Encryption method used as a primary technique for providing the security to information systems. Among all the encryption techniques attribute based encryption (ABE) is getting popularity among the users. For secure data access the client must be sure about the process used for this type of encryption but in cloud platform everything is provided by cloud. Thus the satisfaction of security at user level is not provided by any cloud. Thus this work proposes a novel Client end trust based security service mechanism (TBSSM) using behaviour based encryption for achieving the better results. This work focuses on the application area of cloud storage platform for user satisfaction. This model gives a unique stack based solution for achieving the end user security. In this methodology the attribute can be identified from the user attribute table. This attribute table is dynamic in nature & whose values are passed in the table after a pre calculation of trust & user modelling.

Keywords
CP-ABE(Cipher Text Policy Attribute Based Encryption), KP-ABE (Key Policy attribute Based Encryption), MA-ABE (Multi Authority Attribute Based Encryption),Cloud Platform, ABE (Attribute Based Encryption), TBSSM (Trust Based Security Service Model), Access Policy.

1. INTRODUCTION
Data storage on cloud is provided by the service provider. Storage of this data on un-trusted storage makes secure data sharing a challenging issue. Confidentiality of the data on this unknown environment can be achieved via various access control & encryption mechanism. Conventional encryption standards & techniques will only provide the basic things of security which can be breached. To achieve fine grained access control & effective data access control policies attribute based encryption is well defined standard [1]. There are various encryption algorithms available like AES, 3DES, blowfish etc which will also provide the encryption based security but in a defined manner [2]. It is an burdensome of user to deal with their complex processes. For further improvements in existing methodology of security this work focuses on attribute based encryption with trust value. This paper describe the basic utility of applying attribute based encryption (ABE) for data sharing on un trusted storage & servers.

According to the specified problem the paper gives the solution to the mentioned security issues through TBSSM protocol stack in two steps. In first step, the user focuses on the revocation methodologies based on ABE. It gives the access control mechanism according to the user access historical details. The proposed scheme of TBSSM hides the user's data own policy from itself & the server. In second step the scheme suggest the ABE based unique key generation for encryption & decryption for cloud storage. This key can be generated without the knowledge of accessing profile user & is done by selecting the random attributes from user table.

The primary concern of this work to make the things related to storage more secure without increasing the burden of operating user that is client. After applying the proposed protocol of TBSSM the client can be make the things sure about the security. The TBSSM will also focuses on the parameters of performance which gives the idea that while applying the model complexity can under a certain level. Secure computing environments require flexible access control mechanism. For the large user categories, access control rules for server cannot be uniquely based on individual user identities.

One of the most promising approaches is Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [3]. In this scheme, users possess sets of attributes (and corresponding secret attribute keys) that describe certain properties. Ciphertexts construction assures that only users whose attributes satisfy the access control policy are able to decrypt the ciphertext with their secret attribute keys. Previous attribute based encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in [4], systems attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, the methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC).

It must be impossible for several users to pool their attribute keys such that they are able to decrypt a ciphertext which they would not be able to decrypt individually.

So this paper gives an improved security model TBSSM based on behavioural based encryption with unified trust calculation.

2. BACKGROUND
Emerging cloud technologies will leads towards the big blackouts of unsecured & un-trusted services. It needs to be stimulated with application having flexible access control mechanism & encryption standards. 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]. Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. Access control with a large and dynamic set of users, for objects cannot easily be based on identities. The conditions under which access to an object is granted need to take into account information like the

context and the history of a subject is given by these mechanisms of attributes based encryptions. 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 ciphertext 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 ciphertext 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].

2.1. Attribute Based Encryption

Attribute based encryption is also called as behaviour based encryption (BBE). In this the ciphertext and user keys are associated with policies that describe the user that is allowed to access the encrypted information. Specifically, in Key-Policy ABE (KP-ABE) ciphertext are encrypted with a set of attributes and each user's secret key is associated with a policy describing which ciphertext he can decrypt Figure 1. Such a policy is a predicate over the set of attributes, usually formulated as a Boolean formula [13].

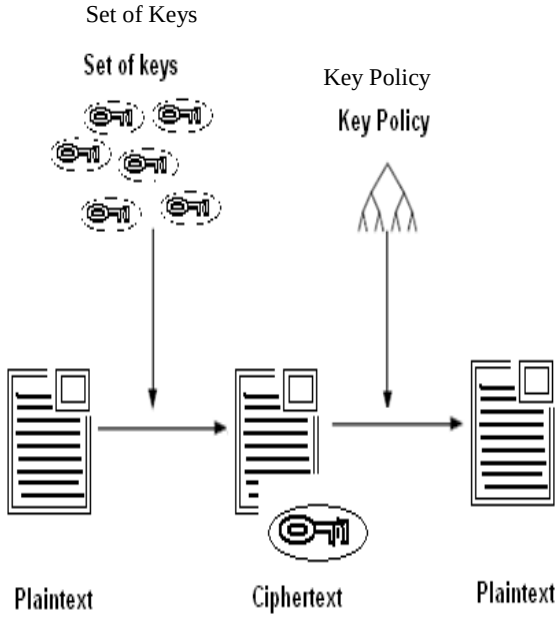

Figure 1:- Schematic diagram of KP-ABE

Conversely, in ciphertext Policy Attribute Based cryptography (CP-ABE) a ciphertext is encrypted with a policy. Anyone whose attributes satisfy the policy will rewrite the ciphertext, otherwise the decoding fails. In a very shell, in CP-ABE a policy is applied throughout cryptography and in KP-ABE a policy is applied throughout decoding [14]. An attribute may be a property or feature that an issue might have. At some purpose in time, any subject might become eligible for a specific attribute, which means that it currently has the individual property or feature. It then receives a token from a trusty party referred to as attribute authority that testifies his eligibility and might be utilized by him to prove that he has the property or feature that the corresponding attribute represents. An attribute is typically delineated as a string. For example, an attribute called is Admin could be used to describe subjects that are administrators of a certain domain. We denote the set of all attributes used in a specific domain as the universe of attributes. In CP-ABE, policies over the universe of attributes are formulated for each object to describe what prerequisites a subject must have to access it.

The attribute based encryption for generating the ciphertext is an extraordinary approach in which user profiles plays an vital role. It gives the access policies for encrypted information. These are mainly used to only generate the key attributes associated with each user & its type of data which it might be access every time. Key Generated Policy Attribute for Encryption (KGPAE) ciphertext are encrypted with a set of attributes and each user's secret key is associated with a policy describing which ciphertext he can decrypt. Such a policy is a predicate over the set of attributes, usually formulated as a Boolean formula. Conventionally this can be achieved by taking the policy for encryption & then generates its cipher values. Similarly anyone whose attributes satisfy the policy can decrypt the ciphertext; otherwise the decryption fails.

An attribute is a property or feature that a subject may have. At some point in time, any subject may become eligible for a particular attribute, meaning that it now has the respective property or feature. It then receives a token from a trusted party called attribute authority that testifies his eligibility and can be used by him to prove that he has the property or feature that the corresponding attribute represents. An attribute is usually represented as a string.

3. LITERATURE SURVEY

The idea of using policies & attributes for encryption was proposed by various researchers. In [7], the author developed a new cryptography algorithm which is based on block cipher concept which uses logical operation like XOR and shifting operation. This technique selects the set of random number for generating the initial key, where this key will use for encrypting the given source file using proposed encryption algorithm with the help of encryption number. Experimental results show that proposed algorithm is very efficient and secured.

To provide better generation & selection of attributes [8] uses modern features in Field Programmable Gate Arrays (FPGA), which allow the modelling of a System on Programmable-Chip (SoPC). Thus the paper proposes a model for symmetric encryption algorithms (e.g., RC5). Structural System analysis of the proposed model shows that it offers extra security against single-site physical access attack that other implementations are vulnerable to. The work has also shown 80% improvement in security.

An efficient encryption technique called quasigroup encryption for encrypting the indexed table is been proposed in [9]. It provides least resemblance of the original data when encrypted. This encryption technique is not efficient in diffusing the statistics of the plain text. This pitfall of quasigroup encryption is further overcome by use of transforms. Hence, this approach uses chained Hadamard

transforms and Number Theoretic Transforms to introduce diffusion along with the quasigroup transformation. The proposed approach is compared with the other encryption approaches and is observed to provide better results. Some of the author carried forward this work for IDS integrated model of Bayes Net with Hidden Markov Model [10].

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. In [14] an extension of RBAC is proposed which allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt.

TAAC (Temporal Attribute based Access Control) a user access control is given in [15]. In it the authorities are independent from each other and no central authority is needed, it is a multi-authority cloud storage system in which the authorities are independent of each other. TAAC can achieve temporal access control on attribute-level rather than on user-level efficiently. Different from the existing schemes with attribute revocation functionality, TAAC does not require re-encryption of any ciphertext when the attribute revocation happens, which means great improvement on the efficiency of attribute revocation. TAAC is highly scalable in nature. Similar to that [16] present a temporal attribute based encryption (TABE) scheme to implement temporal constraints for data access control in clouds. This scheme has a constant size for ciphertext, private-key, and a nearly linear-time complexity. It has four algorithms named as setup, generate key, encrypt & decrypt. At initial level its security model seems to be good & effective.

Similarly DAAC is proposed in [17] which is distributed access control in clouds, where one or more KDCs distribute keys to data owners and users. KDC may provide access to particular fields in all records. Thus, a single key replaces separate keys from owners. Owners and users are assigned certain set of attributes. Owner encrypts the data with the attributes it has and stores them in the cloud. The users with matching set of attributes can retrieve the data from the cloud. Thus various approaches are suggested based on runtime environment to improve the user attribute based encryption performance.

Various other researchers may also focus 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.

4. PROBLEM STATEMENT

During to storing the data at third place client not sure about the information stored safely. There is a 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 this work can get the better results in case of both the types of attribute based encryption KP-ABE [19] & CP-ABE [20]. It needs to keep in concern about the various objectives of data security on this un-trusted server of cloud & storage as given.

The formulated problem has depicted in Figure1

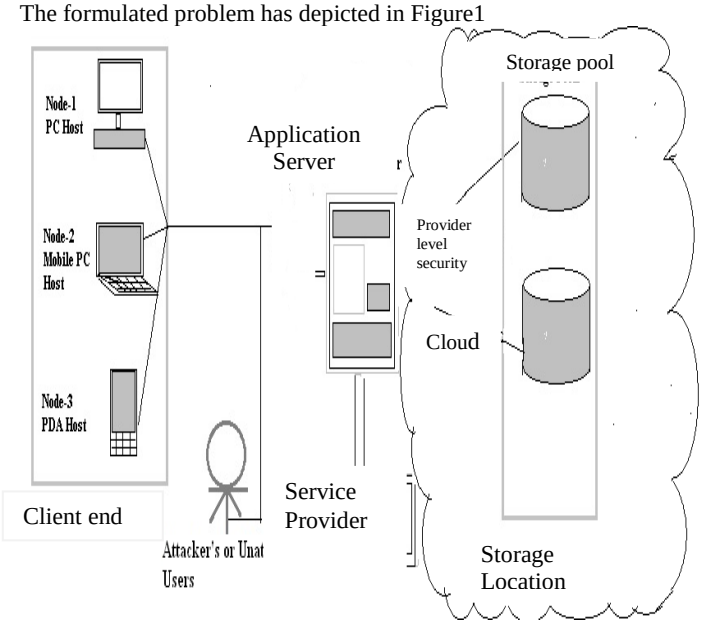

Figure 2:- Data Access by Unauthorized User or Attacker

The above figure 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 in this model to keep data safe from unauthorized access. This model 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; they may collude with other users, or even with the server. 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.

4.1. Security Aims

The security and performance requirements are summarized as follows:

4.1.1 Data confidentiality from unauthorised user's

Users (including the server) who do not have enough attributes satisfying the access policy or who do not have proper key access privileges should be prevented from decrypting a record document, even during user collusion. That means Fine-grained access control should be enforced, that means different users should be authorized to read different sets of documents.

4.1.2 On-*demand revocation for all type of user's*

When a user's attribute is no longer valid, that user should not be able to access future record files by using these attributes. This is usually called attribute revocation.

4.1.3 Write access control from unauthorised users

This approach shall prevent the contributors who are not authorised to gain write-access to owner's record, while the legitimate contributors should access the server with accountability. The access policies of data should be flexible, i.e. dynamic changes to the predefined policies are allowed

4.1.4 The system should be highly scalable, efficient and usable

The system should be supportable for users from both the personal domain and public domains. Since the set of users from the public domain may be large in size and unpredictable, the system should be highly scalable, in terms of complexity in key management, communication, computation and storage. The owners' efforts in managing users and keys should be minimized to enjoy usability.

Our proposed technique of TBSSM can be used for both CP-ABE and KP-ABE and particularly designed for data storage.

5. PROPOSED MECHANISM

Unauthorized access of data, cloud made unreliable for client. To provide reliability on cloud, an approach TBSSM is advised at client end to make safe and secure storage of data. The proposed approach is stack of multiple protections layer that deals with clients' data to providing overlapping layers of authentication, behaviour analysis and make data unreadable form using behaviour based encryption mechanisms. The suggested TBSSM approach consists of several phases.

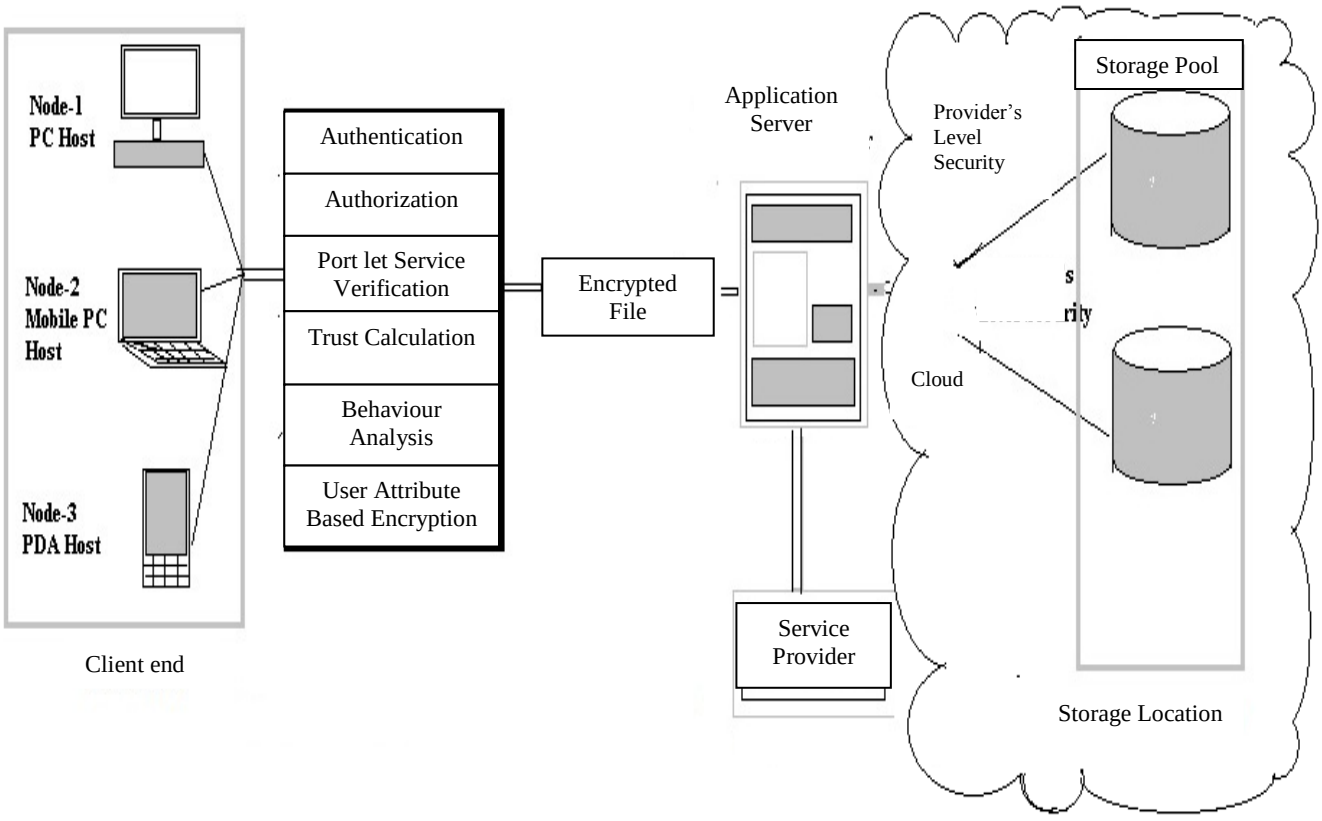

Figure 3:- Proposed Security Stack Protocol

Firstly to coated authentication layer to the data by providing identity of users and verifying the claimed identity. *Secondly* to coated behaviour analysis layer to the data by regular observing the activities of users on the basis of historical property. *Third* phase is to coated behaviour based encryption layer by converting client data into encrypted data and send for storage on the cloud. Figure 3 depicted suggested approach.

The proposed TBSSM model shows stack of protection layer for the client data that are coated in different of phases such as Authentication simply establishes identity, not what that identity is authorized to do or what access privileges he or she has; this is a separate decision related strictly to authorization.

The separation of these three functions (Registration, Authentication and Authorization) by entrusting them to separate entities can be beneficial from a privacy enhancing perspective, as it links and restricts the permissible data processing actions and the availability of personal data to the specific tasks of each actor.

Methodology- Stack approach followed to suggest solution of problem. Different layers of stack protocol coated on the client data one by one to make secure and safe data. It also protects data from unauthorized access.

5.1. TBSSM Stack

5.1.1 Authentication

In this the type of user access & file required is achieved through a authentication phase at application server.

5.1.2 Authorization

The user category & its attribute are authorized from a user database.

5.1.3 Portlet Service verification

In this step the service provided by cloud is verified in browser & gives an identification value of integrity.

5.1.4 Trust Calculation

In this step each user has to reach a unique trust value which is more that a specific threshold which is defined by the user policies. It gives an insight to user activities which is defined after its trust verification.

5.1.5 Behaviour Analysis

The above mentioned trust of every user is analysed by its historical data access & type of files required. It is based on user categorization and access control policies.

5.1.6 User Attribute Based Encryption

It is the final process of TBSSM in which a specific ABE encryption methodology is used to encrypt & decrypt the file for user access. It is based on above trust & behaviour analysis. In this each encryption is done by passing the value of user attribute as a key. In this the size of key is based on number of attribute used.

6. PERFORMANCE EVALUATION

The performance of the proposed approach can be evaluated by some of the basic factors of security. It can be analysed by five specific characteristics of the cloud application at the client end. These are:-

6.1 Security Analysis

In this we measure the security features & properties of our proposed model. In this various other parameters like complexity of key generation, life code, break time etc can be calculated to get accurate analysis.

6.2 *Fine-Grainedness of Access Control*

In this proposed approach of TBSSM, the data origin or creator can define a new access policy based on historical analysis of the behaviour of that user. The size & number of attribute can also be varied. It provides a flexible access to the existing model. Specifically, the access structure of each user is defined as a logic formula over data file attributes, and is able to represent any desired data file set.

6.3 User Access Privilege Confidentiality

Our proposed system just discloses the side node information of a user access tree to Cloud Servers. As internal nodes of an access tree can be any threshold gates and are unknown to Cloud Servers, it is hard for Cloud Servers to recover the access structure and thus derive user access privilege information.

6.4 User Secret Key Accountability

This property can be immediately achieved by using the enhanced construction of CP-ABE to TBSSM which can be used to disclose the identities of key abusers.

6.5 Data Confidentiality

This model analyse data confidentiality in this proposed scheme TBSSM by comparing it with an sensitive scheme in which data files are encrypted using symmetric DEKs, and DEKs are directly encrypted using standard CP-ABE or TBSSM. In this intuitive scheme just ciphertext of data files are given to Cloud Servers. Assuming the symmetric key algorithm is secure.

8. EXPECTED OUTCOMES

Futuristic results of the technique may show the improvement in providing the client level security through cloud environment. 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 TBSSM. At the initial level of our research we get the following benefits.

- It retains reliability on third party location
- Client ensures about data storage in safe manner and unauthorized access.
- It protect data from different attacks at client end
- It might be became innovative approach at client end in cloud platform for different application domains.
- The storage & computation cost can be minimized.
- The attribute encryption gives a wide range for key generation through attribute.
- In this the authentication is achieved in a secure manner.

7. CONCLUSION

This work proposes a novel TBSSM mechanism to increase the security & reliability of the end user to any of the cloud service. A new user always tries to overcome the reliability factors for the data loss. This confidential information will need to be secure & access must be away from security breaches. The TBSSM uses a unique stack based process model which gives security add-ons to the existing methods. It provides the end user security through attribute based encryption (ABE) by which we can pass the file & user attributes as a key during encryption. It will also calculate the trust value of each user before providing any access to any type of data. Moreover, this proposed scheme can enable the data owner to delegate most of computation overhead to powerful cloud servers. Confidentiality of user access privilege and user secret key accountability can be achieved. At initial level this proposed approach seems to be better

secure data access in comparison to other existing methodology.

9. 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 Issue3,2013.