International Journal of Computer Sciences
April'2017 Issue
ISSN Number: 4142 3453

Security Enhancement for Data Sharing On Cloud Using Identity Based Encryption with Revocable Technique

P.S.S. Naveen[1] , P. Prasanna Kumari[2]

[1]M.Tech (CSE)., Dept of CSE,Sri Venkateswara Institute of Science and Technology, kadapa

[2]Assistant Professor, M.Tech., Dept of CSE,Sri Venkateswara Institute of Science and Technology, kadapa

Abstract- Cloud computing is a computing concepts, which enables when required and low maintenance usage of resources, but the data is shares to some cloud servers and various privacy related concerns emerge from it. Various schemes like based on the attribute-based encryption have been developed to secure the cloud storage. Most work looking at the data privacy and the access control, while less attention is given to the privilege control and the privacy. In this paper. InCloud computing as data is outsourced to third party cloud servers, various privacy issues emerge from it which are resolved by various Attribute-Based Encryption schemes. But only decentralized data privacy and privilege control is not important, but user revocation also. In this paper, we present a semianonymous privilege control scheme AnonyControl to address not only the data privacy, but also the user identity privacy in existing access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semianonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Subsequently, we present the AnonyControl-F, which fully prevents the identity leakage and achieve the full anonymity. Our security analysis shows that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie–Hellman assumption, and our performance evaluation exhibits the feasibility of our schemes.

Keywords: Cloud computing, Anonycontrol, Access control, Privilege control, Semi anonymity, fullyanonymity.

1. INTRODUCTION

Cloud computing is a revolutionary computing technique, by which computing resources are provided dynamically via Internet and the data storage and computation are outsourced to someone or some party in a 'cloud'. It greatly attracts attention and interest from both academia and industry due to the profitability, but it also has at least three challenges that must be handled before coming to our real life to the best of our knowledge. First of all, data confidentiality should be guaranteed. The data privacy is not only about the data contents. Since the most attractive part of the cloud computing is the computation outsourcing, it is far beyond enough to just conduct an access control. More likely, users want to control the privileges of data manipulation over other users or cloud servers. This is because when sensitive information or computation is outsourced to the servers might illegally inspect users' data and access sensitive information, or other users might be able to infer sensitive information from the outsourced computation. Therefore, not only the access but also the operation should be controlled. Secondly, personal information (defined by each user's attributes set) is at risk because one's identity is authenticated based on his information for the purpose of access control (or privilege control in this paper). As people are becoming more concerned about their identity privacy these days, the identity privacy also needs to be protected before the cloud enters our life. Preferably, any authority or server alone should not know any client's personal information. Last but not least, the cloud computing system should be resilient in the case of security breach in which some part of the system is compromised by attackers.

Besides these challenges one of the important challenge is attribute revocation over fully anonymous Attribute Based Encryption system like AnonyControl and AnonyControl-F[1].In multiple authority cloud storage systems, each authority can issue attributes independently [2]. There are various schemes which protects privacy of data contents throughattribute based encryption likeIdentity-based encryption (IBE) [3], Fuzzy Identity-Based Encryption, Key-Policy Attribute-Based Encryption (KP-ABE) [4], Ciphertext-Policy Attribute-Based Encryption (CP-ABE)[5].AnonyControland AnonyControl-F [1]which allows cloud servers to not only controluser's access privileges but also protect their identity information.

In the KP-ABE [5], a cipher text is linked with a set of attributes, and a private key is linked with a tree like access structure, which describes this user's identity. Here private key holds the access structure, one can decrypt the cipher text if the access structure in his private key is satisfied by the attributes in the cipher text as cipher text holds attributes.However,private key holds the encryption policy, so the encrypter does not have rights to change the encryption policy[5]. He has to believe that the key generators generate keys with correct access structures to correct users. If a re-encryption occurs, all of the users in the same system must get their private keys re-issued then only they can gain access to the re-encrypted files, and this process causes considerable problems in implementation.

On the other hand, those problems and overhead are all solved in the CP-ABE [5]. In the CP-ABE, cipher texts are linked with an access structure, which gives the encryption policy, and private keys are generated according to users' attributes. A user can decrypt the cipher text if and only if his attributes in the private key satisfy the access tree specified in the cipher text. By doing so, the encrypter holds the ultimate authority about the encryption policy. Also, the already issued private keys will never be modified unless the whole system reboots [11].

Unlike the data confidentiality, less effort is paid to

protectusers' identity privacy during those interactive protocols.Users' identities, which are described with their attributes, aregenerally disclosed to key issuers, and the issuers issue privatekeys according to their attributes. But it seems natural thatusers are willing to keep their identities secret while they stillget their private keys.

ThereforeAnonyControland AnonyControl-F [1]scheme allows cloud servers to controlusers' access privileges without knowing their identity information.The schemes are able to protect user's privacyagainst each single authority.The schemes are tolerant against authoritycompromise, and compromising of up to (N −2) authoritiesdoes not bring the whole system down.

Also user revocation is important issue over fully anonymous system in cloud. This issue is resolved using attribute revocation.Our solution uniquely integrates the proxy re-encryption technique with AnonyControl-F [1], and enables the authority to delegate most delicate tasks of user revocation.

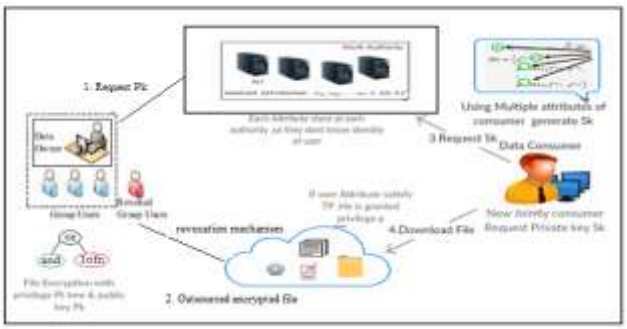

Fig. 1. General Flow of System

II. LITERATURER SURVEY

The concept of ABE for Fine Grained Access Control of Encrypted Data in 2006. He introduces the new cryptosystem for fine grained sharing of encrypted data that is called Key-Policy Attribute-Based Encryption (KPABE). In cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. Fine-grained access control systems facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users. Several techniques are known for implementing fine grained access control. Secret-sharing schemes (SSS) are used to divide a secret among a number of parties. Matthew Pirretti and Brent Waters introduce a novel secure information management architecture based on emerging attribute-based encryption (ABE) primitives also they propose cryptographic optimizations in Secure Attribute Based Systems in 2007. A performance analysis of ABE system and example applications demonstrates the ability to reduce cryptographic costs by as much as 98% over previously proposed constructions. Through this, demonstrates that the attribute system is an efficient solution for securely managing information in large, loosely-coupled, distributed systems. Decryption decrypts a ciphertext encrypted by the Encryption. This process begins with the decrypting party verifying that they have the required attributes. The party performing decryption will then use their attributes to decrypt the decrypt the ciphertext in order to obtain the AES and HMAC key.

John Bethencourt, AmitSahai, Brent Waters introduces Ciphertext-Policy Attribute-Based Encryption in 2008. They employ a trusted server to store the data and mediate access control. In several distributed systems a user should only be able to access data if a user possesses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In addition, they provide an implementation of the system and give performance measurements. The primary challenge in this line of work is to find new systems with elegant forms of expression that produce more than an arbitrary combination of techniques.

Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati describes combination of access control and cryptography in 2010. It illustrates the basic principles on which architecture for combining access control and cryptography can be built. Then illustrate an approach for enforcing authorization policies and supporting dynamic authorizations, allowing policy changes and data updates at a limited cost in terms of bandwidth and computational power. It also described an approach for policy evolution that takes into account the main features of the scenario and is able to guarantee in most cases confidentiality of the information in the presence of significant policy updates, clearly identifying the exposure to collusion when this risk may arise. Other issues to be investigated include the integration with the Web paradigm, and the efficient execution of queries. Markulf Kohlweiss, Ueli Maurer, Cristina Onete, Bjorn Tackmann, Daniele Venturi introduced

Anonymity-preserving Public-Key Encryption: A Constructive Approach where public-key cryptosystems with enhanced security properties have been proposed. it investigate constructions as well as limitations for preserving receiver anonymity when using public-key encryption (PKE). They use the constructive cryptography approach by Maurer and Renner and interpret cryptographic schemes as constructions of a certain ideal resource (e.g. a confidential anonymous channel) from given real resources (e.g. a broadcast channel) and defined appropriate anonymous communication resources and show that a very natural resource can be constructed by using a PKE scheme which fulfills three properties that appear in cryptographic Literature. Results do not only support the trust in existing schemes and constructions; they also show that the simpler and more efficient weakly robust schemes can be used safely.

Junbeom Hur, Dong Kun Noh introduces the concept of Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems in May 16, 2012. The attribute based crypto-systems were introduced such as Ciphertext-Policy Attribute-Base Encryption (CP-ABE) with an addition of two new functions. The first function is KEKGen(U)) which is used to generate keys to encrypt attributes for groups. The other extra function is the ReEncrypt(CT;G) which is a re-encryption that takes the ciphertext and re-encrypt it so that a user in Group G can only access it. R.Ranjith and D.Kayathri Devidescribes the concept of Secure Cloud Storage using Decentralized Access Control with Anonymous Authentication in 2013. It is implemented with secure cloud storage by providing access to the files with the policy based file access using Attribute Based Encryption (ABE) scheme with RSA key public-private key combination.

Private Key is the combination of the user's credentials. So that high security will be achieved. Time based file Revocation scheme is used for file assured deletion. When the time limit of the file expired, the file will be automatically revoked and cannot be accessible to anyone in future. Manual Revocation also supported. Policy based file renewal is proposed. The Renewal can be done by providing the new key to the existing file, will remains the file until the new time limit reaches. Mr. ParjanyaC.A and Mr. Prasanna Kumar describe the concept of Advance Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud in March 2014. They were presented the new framework for MONA. In this method further presented how to manage the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers. This method claims required efficiency, scalability and most importantly reliability. Extensive analyses show that proposed scheme
satisfies the desired security requirements and guarantees efficiency as well. Here it also show that how user gets extra time even after the time out this also one of the advantage of proposed schema. S DivyaBharathy and T Ramesh introduced the concept of privacy preserving access control scheme for data storage, which supports anonymous authentication and performs decentralized key management in Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control in April 2014. In the proposed scheme, the cloud adopts an access control policy and attributes hiding strategy to enhance security. This new scheme supports secure and efficient dynamic operation on data blocks.

III. RELATED WORK

The literature surveys that containing study of different schemes available in Attribute Based encryption(ABE).Those are KPABE, CP-ABE, AnonyControl, AnonyControl–F. Also includes advantage,disadvantage.

A. IBE scheme

Identity-basedencryption (IBE) was first introduced by Shamir [4], inwhich the message sender stipulates an identity suchthat only a message receiver with matching identity can decrypt it.In an Identity-Based Encryption (IBE) scheme [7], the public key of the user is derived from its unique identity, e.g., email address or IP address. The original motivation for identity-based encryption is to help the deployment of a public key infrastructure. Problems with IBE:For sending private key requires secure channel, Private key is known to Private Key Generator (PKG), IBE scheme may depend on cryptographic techniques that are insecure against code breaking attack.

Attribute-Based Encryption (ABE)

Fuzzy Identity-Based Encryption [6], which is also known as Attribute-BasedEncryption (ABE). In such encryption scheme, an identityis viewed as a set of descriptive attributes, and decryption is possible if a descriptor's identity has some overlaps withthe one specified in the ciphertext.Sahai and Waters introduced the first attribute-basedencryption (ABE) [5] where both the cipher text and the secret keyare labeled with a set of attributes[10]. A user can decrypt a cipher textif and only if there is a match between the attributes listedin the cipher text and the attributes held by him. Problems with ABE:The lack of expressibility seems to limit its applicability to larger systems, On demand user revocation and other technique were not adoptable with this encryption method.

Key-Policy Attribute-BasedEncryption (KP-ABE)

In the KP-ABE [6], a ciphertext is associated with aset of attributes, and a private key is associated with amonotonic access structure like a tree, which describes thisuser's identity (e.g. IIT AND (Ph.D OR Master)). A usercan decrypt the ciphertext if and only if the access tree inhis private key is satisfied by the attributes in the ciphertext.Problems with KPABE: Anencryption is the access policy is constructed into user's personal key. So data owner doesnot have the option on who can decrypt the data except encrypting the data with the set of attributes, The data owner is also a trusted authority (TA) at a same time.

Ciphertext-Policy Attribute-BasedEncryption (CP-ABE) Sahai et al [3] introduced the concept of another modified form of ABE called CP-ABE. The key idea of CP-ABE [8] is: the user secret key is associated with a set of attribute and each cipher text will embedded with an access structure. The user can decrypt the message only if the users attribute satisfied with the access structure of the cipher text. CP-ABE [11] improves the disadvantage of KP-ABE that the encrypted data cannot choose who can decrypt it.

While in KP-ABE access policy is associated with private key, while in CP-ABE access policy is associated with cipher text. Problems with CP-ABE:Difficulty in user revocation, Whenever owner wants to change the accessright of user, it is not possible to do efficiently, Decryption keys only support

user attributesthat are organized logically as a single set, so users can only use all possible combination of attributes in a single set issued in their keys to satisfy policies.

AnonyControl and AnonyControl-F

In this paper [1], there are four main roles: N Attribute Authorities (denoted as A), Cloud Server, Data Owners and Data Consumers. Partial information is disclosed in AnonyControland no information is disclosed in AnonyControl- F.

In AnonyControl-F[1] introduced a new technique to let key generators issue the correct attribute key without knowing what attributes the users have. A naive solution is to give all the attribute keys of all the attributes to the key requester and let him pick whatever he wants. In this way, the key generator does not know which attribute keys the key requester picked, but we have to fully trust the key requester that he will not pick any attribute key not allowed to him. To solve this, leverage the Oblivious Transfer (OT) [1].

The KeyGenerate algorithm is the only part which leaks identity information to each attribute authority. Here they have introduced the 1-out-of-n OT to prevent this leakage. They let each authority be in charge of all attributes belonging to the same category. For each attribute category c (e.g., University), suppose there are k possible attribute values (e.g., IIT, NYU, CMU ...), then one requester has at most one attribute value in one category. After the attribute keys are ready, the attribute authority and the key requester are engaged in a 1-out-of-k OT where the key requester wants to receive one attribute key among k. By introducing the 1-out-of-k OT in KeyGenerat algorithm, the key requester achieves the correct attribute key that he wants, but the attribute authority does not have any useful information about what attribute is achieved by the requester. Then, the key requester achieves the full anonymity and no matter how many attribute authorities collude, his identity information is kept secret [1].Problems with

AnonyControl and AnonyControl-F:No User revocation
F. Attribute Based Data Sharing with Attribute Revocation
In this paper [6], author addressed an important issue of attribute revocation for attribute based systems. In particular, they considered practical application scenarios in which semitrustable proxy servers are available, and proposed a scheme supporting attribute revocation. This scheme places minimal load on authority upon attribute revocation events. They achieved this by uniquely combining the proxy re-encryption technique with CPABE and enabled the authority to delegate most laborious tasks to proxy servers. Their proposed scheme is provably secure against chosen ciphertext attacks. Problems with Attribute Based Data Sharing with Attribute Revocation:No data confidentiality,
No privilege control, No identity security

IV. PROPOSED WORK

Propose anonymity Control to allow cloud servers to control users' access privileges without knowing their identity information.

1. The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in anonymity Control and no information is disclosed in anonymity Control-F.

2. The proposed schemes are tolerant against authority compromise, and compromising of up to (N −2) authorities does not bring the whole system down.

3. Provided detailed analysis on security and performance to show feasibility of the scheme anonymity Control and anonymity Control-F.

4. First implement the real toolkit of a multi-authority based encryption scheme anonymity Control and anonymity Control-F.

In this setting, each authority knows only a part of any user's attributes, which are not enough to figure out the user's identity. However, the scheme proposed by Chase considered the basic threshold-based KP-ABE, which lacks generality in the encryption policy expression. Many attribute based encryption schemes having multiple authorities have been proposed afterwards, but they either also employ a threshold-based ABE or have a semi-honest central authority, or cannot tolerate arbitrarily many users' collusion attack.

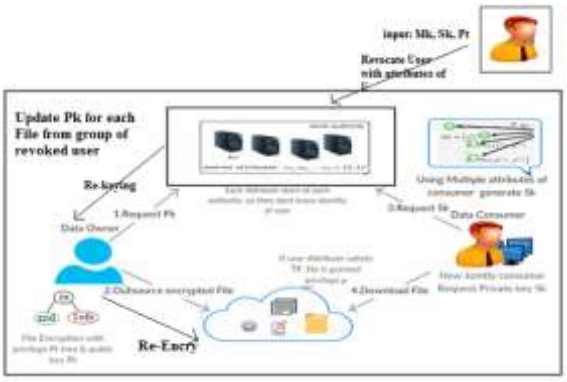

Fig. 2. General Flow of Proposed System

To solve this user revocation problem we proposed attribute revocation for attribute based systems over AnonyControl-F. In this case, we considered real time application scenarios. As shown in Fig. 2 if User1 belongs to c# group of computer department, and User1 is revoked from c# group then public key for each file from revoked user group that is for c# group is updated and updated public key with file name will be sent to the Data owner. Data Owner will encrypt the file with new public key with same access structure and upload on cloud server.

.

V METHODOLOGY

Registration Based Social Authentication Module

The system prepares trustees for a user Alice in this phase. Specifically, Alice is first authenticated with her main authenticator (i.e., password),and then a few(e.g., 5) friends, who also have accounts in the system, are selected by either Alice herself or the service provider from Alice's friend list and are appointed as Alice's Registration.

Security Module Authentication is essential for securing your account and preventing spoofed messages from damaging your online reputation. Imagine a phishing email being sent from your mail because someone had forged your information. Angry recipients and spam complaints resulting from it become your mess to clean up, in order to repair your reputation. trustee-based social authentication systems ask users to select their own trustees without any constraint. In our experiments (i.e., Section VII), we show that the service provider can constrain trustee selections via imposing that no users are selected as trustees by too many other users, which can achieve better security guarantees. 5.3Attribute based encryption Attribute-based encryption module is using for each and every node encrypt data store. After encrypted data and again the re-encrypted the same data is using for fine-grain concept using user data uploaded. the attribute-based encryption have been proposed to secure the cloud storage. Attribute-Based Encryption (ABE). In such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a decrypter's identity has some overlaps with the one specified in the ciphertext. 5.4Multi-authority A multi-authority system is presented in which each user has an id and they can interact with each key generator (authority) using different pseudonyms. Our goal is to achieve a multi-authority CP-ABE which achieves the security defined above; guarantees the confidentiality of Data Consumers' identity information; and tolerates compromise attacks on the authorities or the collusion attacks by the authorities. This is the first implementation of a multi-authority attribute based encryption scheme.

VI. RESULT AND DISCUSSIONS

The implementation can be gone through in a stage-wise method as follows. Fig. 3 shows the computation overhead incurred in thecore algorithms Setup, KeyGenerate, Encrypt, and Decryptunder various conditions. We additionally taken just their results from papersthreesimilar works (Li [12], Muller [13], and Chase [12]) under thesame condition (same security level and same environment) forthe comparison purpose and base paper [1].

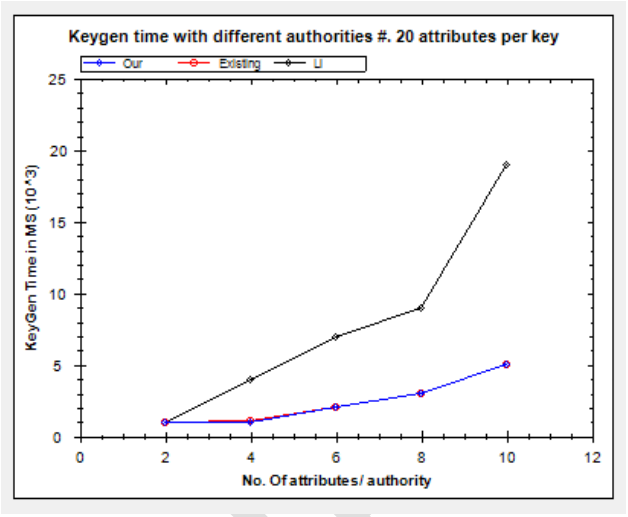

Fig. 3. Keygen time with different authorities (20 attributes per

key) Particularly, in Fig. 3, we have plotted graph for measuring key generation time with different authorities (20 attributes per key) and in Fig. 4 we are measuring key generation time with Jdifferent attributes #. (5 authorities)

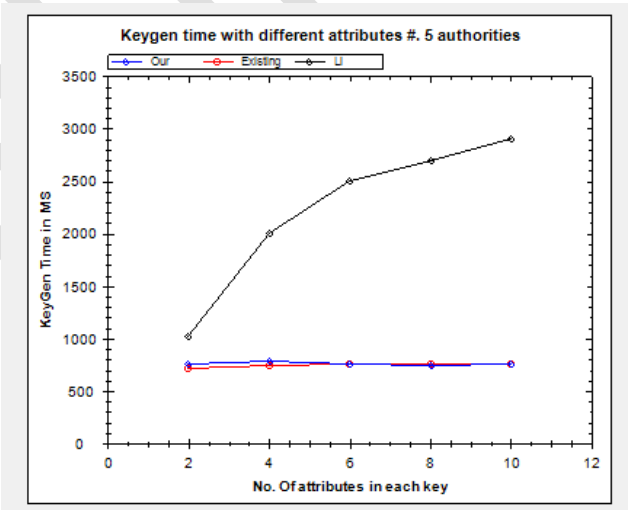

Fig. 4. Key generation time with different attributes #. 5 Authorities

VII.CONCLUSION

This paper proposes a semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users' identity information.In Cloud computing system for multiple authorities, our proposed schemes achieve not only fine-grained privilege control and identity privacy but also user revocation using attribute revocation schemeover AnonyControl-F scheme which is can tolerate up to N − 2 authority compromise. Future scope of our scheme is to

reduce communication overhead in this user revocation over AnonyControl-F system.

REFERENCE

[1]. B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski,R. Kemmerer, C. Kruegel, and G.Vigna, "Your botnet is my botnet: Analysis of a botnet takeover," in CCS '09: Proceedings of the 2009 ACM conference on computer communication security, 2009.

[2]. D. Dagon, C. Zou, andW. Lee, "Modeling botnet propagation using time zones," in Proceedings of the 13 th Network and Distributed System Security Symposium NDSS, 2006.

[3]. M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "My botnet is bigger than yours (maybe, better than yours): why size estimates remain challenging," in Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets, 2007.

[4]. D. Dagon, C. C. Zou, and W. Lee, "Modeling botnet propagation using time zones," in NDSS, 2006.

[5]. P. V. Mieghem, J. Omic, and R. Kooij, "Virus spread in networks," IEEE/ACM Transactions on

Networking, vol. 17, no. 1, pp. 1–14, 2009.

[6]. Cabir, http://www.f-secure.com/en/web/labs global/2004- threat-summary.

[7]. S. Peng, S. Yu, and A. Yang, "Smartphone malware and its propagation modeling: A survey," IEEE

Communications Surveys and Tutorials, in press, 2014.

[8]. Z. Chen and C. Ji, "An information-theoretic view of network-aware malware attacks," IEEE Transactions

on Information Forensics and Security, vol. 4, no. 3, pp. 530– 541, 2009.

[9]. A.M. Jeffrey, xiaohua Xia, and I. K. Craig, "When to initiate hiv therapy: A control theoretic approach,"

IEEE Transactions on Biomedical Engineering, vol. 50, no. 11, pp. 1213–1220, 2003.

[10]. R. Dantu, J.W. Cangussu, and S. Patwardhan, "Fast worm containment using feedback control," IEEE

Transactions on Dependable and Secure Computing, vol. 4, no. 2, pp. 119–136, 2007.

[11]. S. H. Sellke, N. B. Shroff, and S. Bagchi, "Modeling and automated containment of worms," IEEE Trans.

Dependable Sec. Comput., vol. 5, no. 2, pp. 71–86, 2008.

[12]. P. De, Y. Liu, and S. K. Das, "An epidemic theoretic framework for vulnerability analysis of broadcast

protocolsin wireless sensor networks," IEEE Trans. Mob. Comput., vol. 8, no. 3, pp. 413–425, 2009.

[13]. G. Yan and S. Eidenbenz, "Modeling propagation dynamics of bluetooth worms (extended version),"

IEEE Trans. Mob. Comput., vol. 8, no. 3, pp. 353–368, 2009.

[14] h. Ma, g. Zeng, z. Wang, and j. Xu, "fully secure multi-authority Attribute-based traitor tracing," j. Comput. Inf. Syst., vol. 9, no. 7, Pp. 2793–2800, 2013.

[15] s. Hohenberger and b. Waters, "attribute-based encryption with Fast decryption," in public-key cryptography. Berlin, germany: Springer-verlag, 2013, pp. 162–179.

[16] j. Hur, "attribute-based secure data sharing with hidden policies in smart Grid," ieee trans. Parallel distrib. Syst., vol. 24, no. 11, pp. 2171–2180, Nov. 2013.

[17] y. Zhang, x. Chen, j. Li, d. S. Wong, and h. Li, "anonymous attribute based Encryption supporting efficient decryption test," in proc. 8th Asiaccs, 2013, pp. 511–516. [18] d. Boneh and m. Franklin, "identity-based encryption from the weil Pairing," in advances in cryptology. Berlin, germany: springer-verlag, 2001, pp. 213–229.

[19] a. Sahai and b. Waters, "fuzzy identity-based encryption," advances In cryptology. Berlin, germany: springer-verlag, 2005.

[20] j. Liu, z. Wan, and m. Gu, "hierarchical attribute-set based encryption For scalable, flexible and fine-grained access control in cloud computing," In information security practice and experience.berlin,germany: Springer-verlag, 2011, pp. 98–107.

AUTHORS PROFILE

Mr. S. Naveen, pursuing M.Tech., (CSE) at Sri Venkateswara Institute of Science and Technology, Kadapa.

Smt. P. Prasanna Kumari, M.Tech., (CSE) Assistant Professor at Sri Venkateswara Institute of Science and Technology, kadapa.