iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5481

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Preventing unauthorized Data Access in Fully Obscure Attribute Based Encryption with Security Solutions

Snehanka Patil [1], Manjusha Tatiya [2]
[1]*P.G. Student, Department of Computer Engineering, Indira College of Engineering, Savitribai Phule Pune ,University, Maharashtra, India*[1]
[2]*Professor, Department of Computer Engineering, Indira College of Engineering, Savitribai Phule Pune ,University, Maharashtra, India*[2]

Abstract*: *Now days all over world everyone is connected to internet, that main reason to provide security to their data its most important things. Message transmission as well as stored on particular station also accessing them it main agenda, for data storing many tools available like fog computing cloud computing etc. Cloud computing may perhaps be a revolutionary computing is typical pattern, that allows versatile, on-demand, and cheap usage of computing resources, however the knowledge is outsourced to some cloud servers, and varied privacy problems emerge from it. Numerous schemes supported the attribute-based secret writing square measure projected to secure the cloud storage. However, most work focuses on the knowledge contents privacy so the access management, whereas less attention is paid to the privilege management so the identity privacy. Throughout this paper, we have associate inclination to gift a semi anonymous privilege management theme AnnonyControl to handle not solely the information privacy, however conjointly the user identity privacy in existing access management schemes. Annony management decentralizes the central authority to limit the identity run so achieves semi namelessness. Besides, it conjointly generalizes the file access management to the privilege management, by that privileges of all operations on the cloud info could also be managed in Associate in Nursing passing fine-grained manner. Afterwards, we tend to gift the Annony Control-F, that fully prevents the identity outflow and succeed the entire obscurity. Our security analysis shows that each Annony management and AnnonyControl-F unit secure below the decisional linear Diffie–Hellman assumption, and our performance analysis exhibits the utility of our schemes.

Keywords: ***AnonyControl, Attribute-based secret writing, behaviour profiling, decoy, multi-authority, obscure***

I. INTRODUCTION

Online Businesses, particularly start-ups, little and medium businesses, square measure more and more choosing outsourcing information and computation to the Cloud. This clearly supports higher operational potency, however comes with larger risks, perhaps the most serious of that is information stealing attacks. Data stealing attacks square measure amplified if the aggressor may be a malicious insider. This is often thought of collectively of the highest threats to cloud computing by the Cloud Security Alliance. While most cloud computing customer's square measure well-aware of this threat, they are left solely with trusting the service supplier once it comes to protective their information. The dearth of transparency into, let alone management over, the Cloud provider's authentication, authorization, and audit controls solely exacerbates this threat. The Twitter incident is one example of an information stealing attack from the Cloud. Many Twitter company and private documents were ex-filtrated to technological web site TechCrunch , and customers' accounts, as well as the account of U.S. President Barack Obama, were illicitly accessed. The aggressor used a Twitter administrator's password to realize access to Twitter's company documents, hosted on Google's infrastructure as Google Docs. The damage was important each for Twitter and for its customers. While this explicit attack was launched by AN outsider, stealing a customer's admin passwords is way easier if perpetrated by a malicious corporate executive. Rocha and Correia define how straightforward passwords could also be purloined by a malicious corporate executive of the Cloud service supplier. The authors additionally incontestable how Cloud customers' non-public keys may be purloined, and how their confidential information may be extracted from a tough disk. After stealing a customer's secret and personal key, the malicious corporate executive get access to all or any client information, while the customer has no means that of police work this unauthorized access. However, these mechanisms haven't been ready to prevent information compromise [1]. After considering all these information we propose some new approach to provide security for data. In this paper provide information regarding data

securing on internet as well as to alerts message to user of that intruder via email. Our system provides access only for particular users which grant by authorized user in particular filed.

II. LITERATURE SURVEY

[2] In this paper they have a tendency to introduce a unique sort of cryptanalytic theme, that allows any try of users to speak firmly and to verify every other's signatures while not exchanging non-public or public keys, while not keeping key directories, and while not exploitation the services of a third party.

For storage is used passionately for on-line information storage. Cipher text Policy-Attribute based secret writing (CP-ABE) is taken under consideration because the promising declare information access management for the outsourced information detain the cloud servers as a result of the user satisfying the access structure can entirely access the encrypted information[3].

Ciphertext-Policy

Attribute primarily based encoding (CP-ABE) could be a promising cryptologic primitive for fine-grained access management of shared knowledge. In CP-ABE, every user is related to a group of attributes and knowledge square measure encrypted with access structures on attributes. A user is in a position to rewrite a ciphertext if and provided that his attributes satisfy the ciphertext access structure [4].

In [5] and [6], a multi-authority system is given inside that every user has associate ID (GID) that they will act with every key generator(authority) exploitation absolutely altogether totally different pseudonyms. One user's altogether totally different pseudonyms unit of measure tied to his personal key, but key generators ne'er comprehend the non-public keys, then they don't seem to be able to link multiple pseudonyms happiness to identical user.

Also, the whole attributes set is split into N disjoint sets and managed by N attributes authorities. throughout this setting, every authority is awake to alone a selected region of any user's attributes, that don't seem to be enough to work out the user's identity. However, the theme projected by Chase et al.

[6] thought-about the essential threshold-based KP-ABE, that lacks generality at intervals the cryptography policy expression. several attribute primarily based cryptography schemes having multiple authorities area unit came into the image later [7]–[10], however they either as well use a threshold-based ABE [7], or have a semi-honest central authority [8]–[10], or cannot tolerate several users' collusion attack [7].

The add [11] and [12] unit of measure the foremost similar ones to ours throughout this they as well tried to alter the central authority at intervals the CP-ABE into multiple ones. A LSSS matrix is used as associate access structure, but their theme alone converts the AND, OR gates to the LSSS matrix, that limits their cryptography policy to Boolean formula, whereas we tend to tend to inherit the physical property of the access tree having threshold gates.

Muller et al. as well supports alone reciprocally exclusive ancient sort (DNF) in their cryptography policy. Besides the actual undeniable fact that we tend to tend to square measure able to specific haphazardly general cryptography policy, the system as well tolerates the compromise attack towards attributes authorities, that will not lined in several existing works. Recently, there as well appeared traceable multi-authority ABE [13] and [14].

Those schemes introduce responsibility specific malicious users' keys square measure sometimes derived. On the alternative hand, in similar direction as this method is usually found in [15]–[16], administrative body attempt to hide cryptography policy at intervals the ciphertexts, however their solutions reveal the attribute at intervals the key generation 0.5.

III.SYSTEM OVERVIEW

Our system contains four sorts of entities: N Attribute Authorities (denoted as A), Cloud Server, data homeowners and knowledge customers. A user is also an information Owner and a information shopper at identical time. Authorities square measure assumed to possess powerful computation skills, which they're supervised by government offices as a results of some attributes partially contains users' nose to nose recognizable knowledge. the complete attribute set is split into N disjoint sets and controlled by each authority, so each authority is awake to alone a region of attributes.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

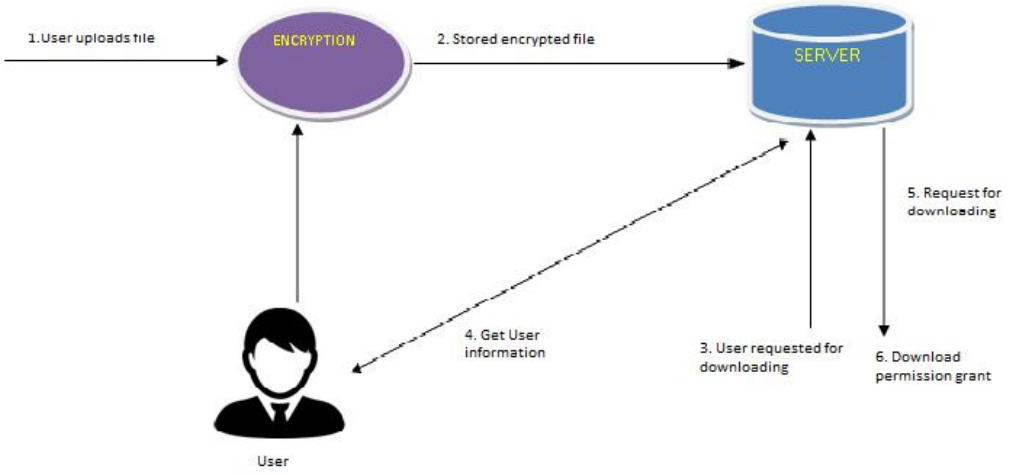


Fig. 1 System Diagram

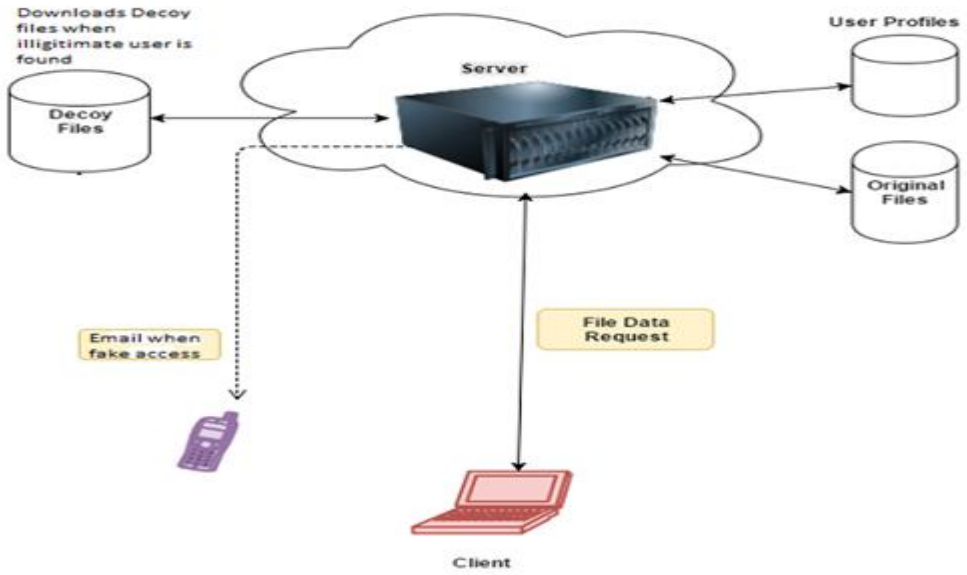


Fig. 2 General Idea of system

A. System Model

The In our system, there are four sorts of entities: N Attribute Authorities (denoted as A), Cloud Server, data householders and knowledge customers. Users are usually a information Owner and a information shopper at a similar time. Authorities are assumed to have powerful computation skills, which they're supervised by government offices as results of some attributes part contain users' face to face identifiable data. The complete attribute set is split into N disjoint sets and controlled by each authority, thus each authority is aware of alone an area of attributes. a knowledge Owner is that the entity international organization agency has to supply encrypted record to the Cloud Servers. The Cloud Server, United Nations agency is assumed to have adequate storage capability, will nothing but store them. new joined data customers request private keys from all of the authorities, which they do not apprehend that attributes are controlled by that authorities. Once the knowledge customers request their private keys from the authorities, authorities collectively turn out corresponding private key and send it to them. All data customers are able to transfer any of the encrypted data files, but alone those private keys satisfy the privilege tree Tp can execute the operation associated with privilege p. The server is delegated to execute associate operation p if and given that the user's credentials are verified through the privilege tree Tp.

B. Threats Model

We assume the Cloud Servers are semi-honest, World Health Organization behave properly in most of sometime but would possibly conspire with malicious data shoppers or data householders to reap others' file contents to realize illegitimate profits. But are put together assumed to comprehend legal profit once users' requests are properly processed, which suggests they will follow the protocol ordinarily. N authorities are assumed to be untreated. That is, they'll follow our planned protocol ordinarily; however attempt to establish the most quantity knowledge as realizable severally. a lot of specifically, we tend to tend to assume they are interested by users' attributes to realize the identities, but they will not conspire with users or different authorities. This assumption is analogous to many previous researches on security issue in cloud computing (see [20], [29]–[31]), and it's put together low cost since these authorities are getting to be audited by government offices. However, we are going to any relax this assumption and allow the collusion between the authorities in Section VI. Knowledge shopper's square measure untreated since they are random users together with attackers. They'll move with different data shoppers to illegally access what they don't seem to be allowed to. Besides, we tend to tend to do not take under consideration the identity outpouring from the underlying network since this may be trivially prevented by using anonym zed network protocols.

C. AnonyControl Construction

To formally define the protection of our AnnonyControl, we tend to initial offer the following definitions. Setup → PK, MKk: This rule takes nothing as input except implicit inputs like security parameters. Attributes authorities execute this rule to jointly cypher a system-wide public parameter PK equally as degree authority-wide public parameter yk, and to one by one cypher a key MKk. Key Generate(PK, MKk, Au) → SKu: This rule permits a user to maneuver with every attribute authority, and obtains a private key SKu like the input attribute set Au. Encrypt(PK, M, p∈)→ (CT, VR): This rule takes as input the final public key PK, a message M, and a collection of privilege trees p∈, where r is about by the encrypter. can} inscribe the message M and returns a ciphertext CT and a verification set VR so as that a user will execute specific operation on the ciphertext if and providing his attributes satisfy the corresponding privilege tree Tp. As we tend to outlined, T0 stands for the privilege to browse the file. decipher (PK, SKu, CT) → M or verification parameter: This rule area unit progressing to be used at file dominant (e.g. reading, modification, deletion). It takes as input the final public key PK, a ciphertext CT, and a private key SKu, that contains a collection of attributes Au and corresponds to its holder's GIDu. If the set Au satisfies any tree at intervals the set p∈, the rule returns a message M or a verification parameter. If the verification parameter is successfully verified by Cloud Servers, WHO use VR to verify it, the operation request area unit progressing to be processed. Next, we tend to tend to stipulate the protection of our AnonyControl with the subsequent game. Init: The somebody A declares the set of compromised authorities ⊂ A (where a minimum of two authorities terribly} very aren't management diode by A) that unit of measurement below his management (remaining authorities A/ unit of measurement controlled by the challenger). Then, he declares T0 that he needs to be challenged, throughout that some attributes unit of measurement being in charged by the challenger's authorities. Setup∗: The competitor and so the somebody jointly run the Setup rule to receive the valid outputs. section 1: The somebody launches Key Generate algorithms to question for as many personal keys as he needs, that correspond to attribute sets A1,. . ., Aq being disjointly in charged by all authorities , but none of these keys satisfy T0. Besides, he jointly conducts at random many computations practice the general public and secret keys that he has (belonging to compromised authorities). Challenge: The somebody submits two messages M0 and M1 of equal size to the competitor. The competitor flips a random binary coin b and encrypts Mb with T0. The ciphertext CT is given to the somebody. section 2: half one is continual adaptively, but none of the queried keys satisfy T0. Guess: The somebody outputs a guess b of b. The advantage of degree somebody A throughout this game is made public as Pr[b = b] − one 2 . Definition 2: Our theme is secure and indistinguishable against chosen-attribute attack (IND-CAA) if all probabilistic polynomial-time adversaries (PPTA) have at the foremost a negligible advantage at intervals the on high of game. Note that the IND-CAA printed on high of implies IND-CCA since the somebody can conduct encryptions and decryptions practice the final public keys and secret keys it owns in section one and half 2 (but he cannot rewrite the target ciphertext since none of its secret keys satisfy T0).

D. Style Goal

Our goal is to comprehend a multi-authority CP-ABE which: achieves the protection printed above; guarantees the confidentiality of data Consumers' identity information; and tolerates compromise attacks on the authorities or the collusion attacks by the authorities. For the visual comfort, we tend to frequently use the following notations hereafter. Province denotes the k-th attribute authority; Au denotes the attributes set of user u; Au k denotes the set of Au controlled by Ak; and ATP denotes the attributes set enclosed in tree Tp.

In previous system for network security it can be used decoy system here come another question come in mind what is decoy and how it work? The construct of Decoy Systems isn't new the network security world, as geological formation Stoll first delineates it in his book entitled "The Cuckoo's Egg."1 Stoll delineate a jail-type technology that captured associate degree unauthorized users access to a system to work out his intentions. it's only in the near past that the construct has been adopted by the plenty for production implementation to help in a very defensive network security posture. A compromised decoy system offers a wealth of options that may assist with intelligence data gathering, incident response and network forensics, for a more robust understanding of who the offender is, what methodology the offender accustomed gain access and therefore the results of the attacker's unauthorized attack for doable prosecution measures.

These options include suspicious event alerts to a management digital computer for visual and hearable notification, the flexibility to capture the unauthorized user's keystrokes and send it to a remote syslog server, varied custom-built work and imitative system files and information to possess the unauthorized user waste time because the security administrator prepares a measure. Several merchandise area unit on the market to help in making a decoy system, every of that has its own interpretation of what a decoy system is and the way it ought to be used. The general process of putting in decoy systems on a network infrastructure is comparatively easy. The main parts area unit unremarkably an additional interface on the firewall to regulate knowledge communications and also the deception system. In selecting a variety of decoy system, an organization's defense posture and money scenario should be taken into thought. For example, Symantec's ManTrap and search software system (formerly Recourse Technologies) may be a commercially on the market product that depicts a variety of decoy system. ManTrap accomplishes this task by running a picture of AN package at intervals another package, whereas search makes an attempt to find the unauthorized user. ManTrap collects proof necessary for prosecution and makes hackers believe they are offensive very important info systems. This approach assists in maintaining network performance by protective the network and collection logs while not impeding legitimate traffic. ManTrap can log all keystrokes, processes, and files accessed throughout every attack. The ManTrap decoy system conjointly uses a hardware token to digitally sign and time stamp log files to ensure non-repudiation within the event they're required for prosecution or legal actions. search and ManTrap merchandise supply intensive client support and carry a fashionable tag.

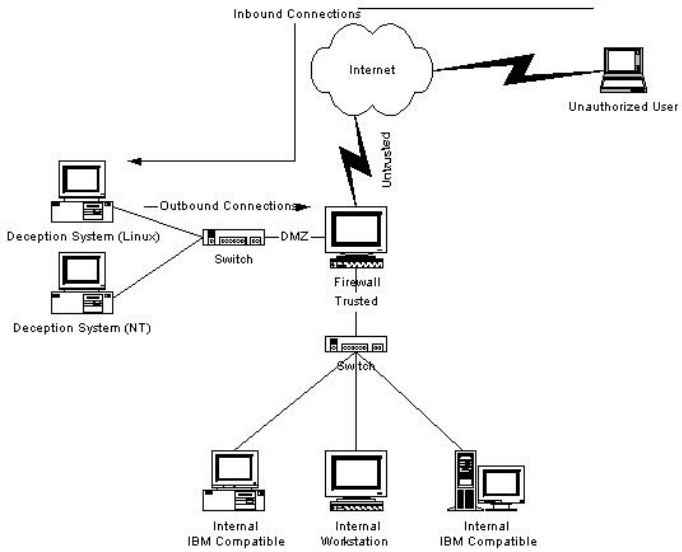


Fig. 3 Data Control of Decoy Systems on a Separate Network

The use of deception can aid in drawing the unauthorized user's attention from the trusted network to the decoy network. there's associate degree assortment of common schemes for deploying decoy systems. the primary means is to form a separate network, ideally on a demilitarized zone (DMZ), and therefore the alternative relies on "The Minefield" principle wherever the decoy systems area unit amalgamated with the assembly systems. Decoy systems placed on a DMZ to lure attackers aloof from the interior trusty network assets offer several advantages, as illustrated in Figure one. associate degree access management rule set on the firewall will be less demanding on the DMZ network wherever the decoy systems reside. once the unauthorized user performs scans to find system vulnerabilities, the decoy systems on the network would reply and move all focus aloof from the trusty network resources. Another thing also we that whenever two system find some suspicious thing is happing when doing then system can alerts users via

giving particular message its call as system behaviour . In another word system can check the behaviour of overall system and if it find something wrong that is which is not set on its protocols then it can alert user and block that intruder. But main problem is that above two methods which can provide security to user they used in separately so its effect is not so much affective. So basic aim behind our system is that after combining these two different concept and increased its performance and give more security to our system as shown in figure below.

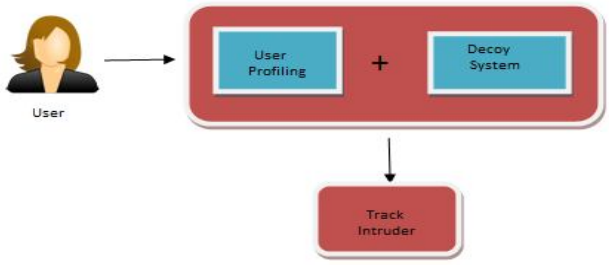


Fig. 4 Combined Approach of Security

The decoy system and behaviour profiling secure the system in their own way. But when these both techniques are used together provides more security. The result analysis given below shows how it gives better result.

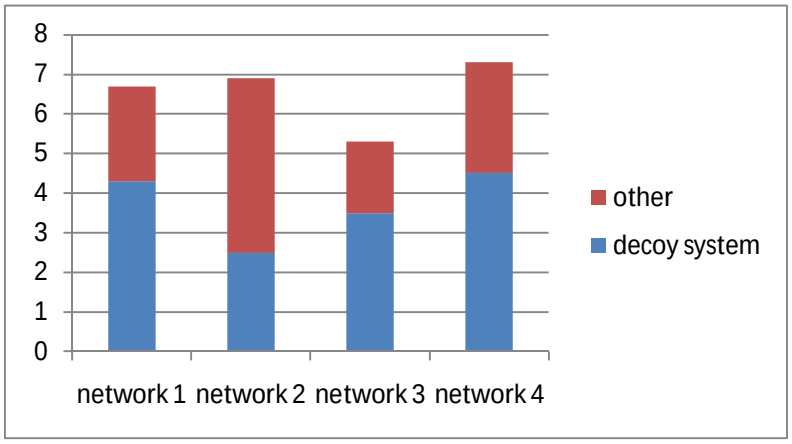


Fig. 5.Graph of comparison between decoy and other systems

Line graph show the decoy system work separately on differ types of network with other security which provide by its owner to it. Similarly when system behaviour when work on separately

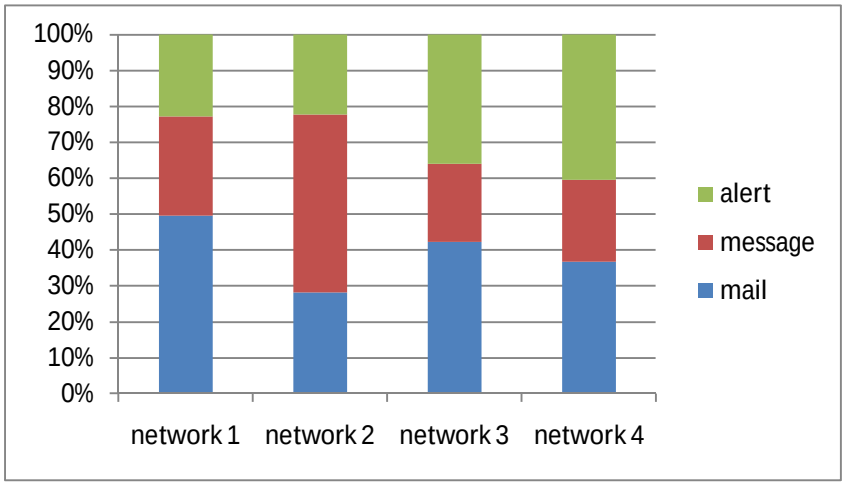


Fig. 6.Graph of behaviour profiling result

But when ever these two systems combined then system get stronger. This system gives better result as many security solutions have been provided.

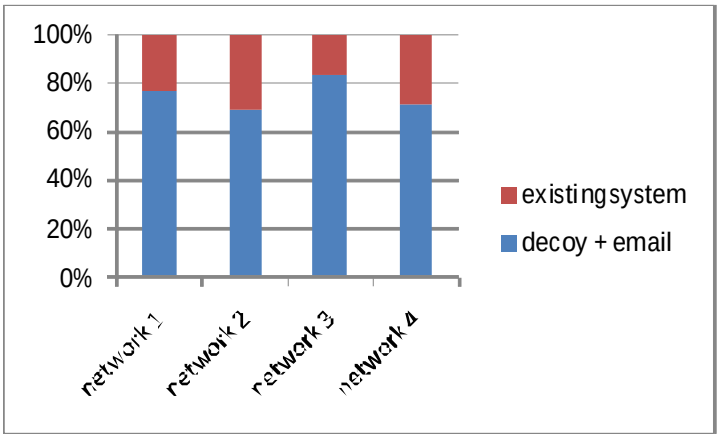


Fig. 6.Graph existing system vs decoy system and email security

IV. CONCLUSIONS

In this approach, we have a tendency to find abnormal search and decoy traps along for a good masquerade detection system. Combining the two techniques improves finding accuracy and provides distinctive levels of security to detect business executive felony attacks. we have a tendency to apply these ideas to find illegitimate knowledge access to knowledge hold on a neighborhood file system by masqueraders, i.e. Attackers World Health Organization cause as legitimate users when stealing their credentials. once a villain business executive tries to use the Cloud for knowledge dynamics, he gets drawn to bastard data that seems sensitive and helpful to hackers. Manner this fashion the projected application deceives malicious users to behave that way and avoid business executive felony attack. Our experimental results in a native file system setting show that combining each technique will yield higher detection results and our results counsel that this approach may fit in a Cloud setting, as the Cloud is supposed to be as clear to the user as a native file system. during this approach, we have a tendency to find abnormal search and decoy traps along with a good masquerade detection system. Combining the two techniques improves detection accuracy.

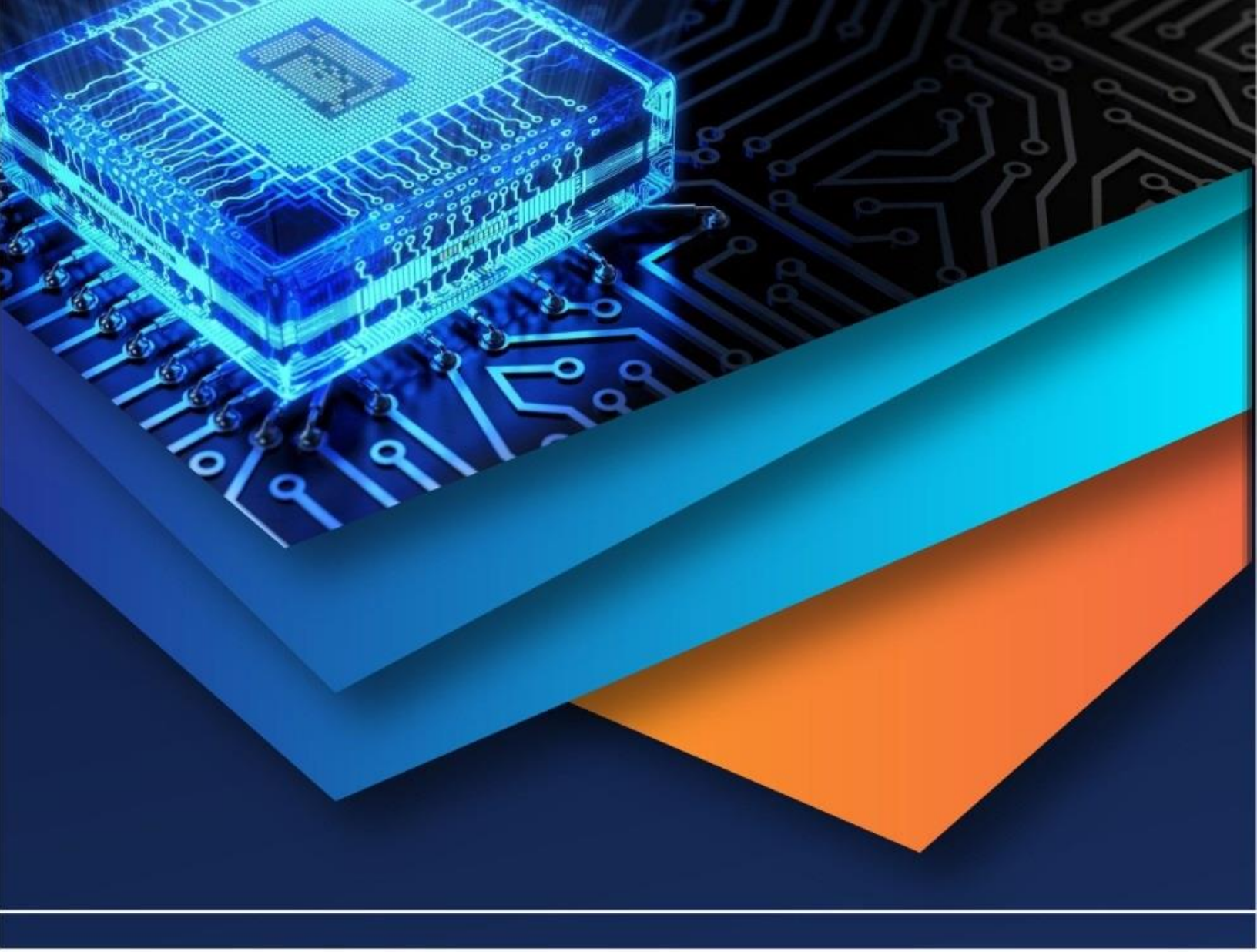
V. ACKNOWLEDGMENT

I would prefer to categorical my feeling to a prof. Manjusha Tatiya for providing maine adequate facilities to complete this paper. I categorical my feeling for her support and suggestions relating to the thesis. I additionally convey Department of computer engineering for support and encouragement.

REFERENCES

[1] Shamir, “identity-based cryptosystems and signature schemes,” in advances in cryptology.berlin,germany:springer-verlag,1985,pp.47–53
[2] A. Sahai and b. Waters, “fuzzy identity-based encryption,” in advances in cryptology. Erlin,germany:springer-verlag,2005,pp.457–473
[3] V. Goyal, o. Pandey, a. Sahai, and b. Waters, “attribute-based encryption for fine-grained access control of encrypted data,” in proc. 13th ccs, 2006, pp. 89–98
[4] J. Bethencourt, a. Sahai, and b. Waters, “ciphertext-policy attributebased encryption,” in roc. Ieee sp, may 2007, pp. 321–334.
[5] M. Chase, “multi-authority attribute based encryption,” in theory of cryptography. Berlin, germany: springer-verlag, 2007, pp. 515–534.
[6] M. Chase and s. S. M. Chow, “improving privacy and security in multi-authority attribute based encryption,” in proc. 16th ccs, 2009, pp. 121–130
[7] H. Lin, z. Cao, x. Liang, and j. Shao, “secure threshold multi authority attribute based encryption without a central authority,” inf. Sci., vol. 180, no. 13, pp. 2618–2632, 2010
[8] V. Božovi´ c, d. Socek, r. Steinwandt, and v. I. Villányi, “multi-authority attribute-based encryption with honest-but-curious central authority,” int. J. Comput. Math., vol. 89, no. 3, pp. 268–283,2012
[9] F. Li, y. Rahulamathavan, m. Rajarajan, and r. C.-w. Phan, “low complexity multi-authority attribute based encryption scheme for mobile cloud computing,” in proc. Ieee 7th sose,-mar.2013,pp.573–57
[10] K. Yang, x. Jia, k. Ren, and b. Zhang, “dac-macs: effective data access control for multi-authority cloud storage systems,” in proc. Ieee infocom, apr. 2013, pp. 2895–2903 ieee transactions on information forensics and security, vol. 10, no. ,january-2015 june et al.:control cloud data access privilege and anonymity-19
[11] A. Lewko and b. Waters, “decentralizing attribute-based encryption,” in advances in cryptology.berlin,germany:-springer-verlag-2011,pp.-568–588
[12] S. Müller, s. Katzenbeisser, and c. Eckert, “on multi-authority ciphertext-policy attribute-based encryption,” bull. Korean math. Soc., vol. 46, no. 4, pp. 803– 819, 2009

[13] J. Li, q. Huang, x. Chen, s. S. Chow, d. S. Wong, and d. Xie, "multiauthority ciphertext-policy attribute-based encryption with accountability," in proc. 6th asiaccs, 2011, pp. 386–390
[14] H. Ma, g. Zeng, z. Wang, and j. Xu, "fully secure multi-authority attribute-based traito 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. 201
[17] y. Zhang, x. Chen, j. Li, d. S. Wong, and h. Li, "anonymous attributebased 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. 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.
[20] A. Kapadia, p. P. Tsang, and s. W. Smith, "attribute-based publishing with hidden credentials and hidden policies," in proc. Ndss, 2007, pp. 179–192.
[21] S. Yu, k. Ren, and w. Lou, "attribute-based content distribution with hidden policy," in proc. 4th workshop secure netw. Protocols, oct. 2008, pp. 39–44.
[22] Z. Wan, j. Liu, and r. H. Deng, "hasbe: a hierarchical attributebased solution for flexible and scalable access control in cloud computing," ieee trans. Inf. Forensics security, vol. 7, no. 2, pp. 743–754, apr. 2012.
[23] T. Jung, x. Mao, x.-y. Li, s.-j. Tang, w. Gong, and l. Zhang, "privacypreserving data aggregation without secure channel: multivariate polynomial evaluation," in proc. Ieee infocom, apr. 2013, pp. 2634–2642.
[24] T. Jung and x.-y. Li, "collusion-tolerable privacy-preserving sum and product calculation without secure channel," ieee trans. Dependable secure comput.,to be published.
[25] [26] x.-y. Li and t. Jung, "search me if you can: privacy-preserving location query service," in proc. Ieee infocom, apr. 2013, pp. 2760–2768.
[26] L. Zhang, x.-y. Li, y. Liu, and t. Jung, "verifiable private multiparty computation: ranging and ranking," in proc. Ieee infocom, apr. 2013, pp. 605–609
[27] L. Zhang, x.-y. Li, and y. Liu, "message in a sealed bottle: privacy preserving friending in social networks," in proc. Ieee 33rd icdcs, jul. 2013, pp. 327– 336.
[28] C. Wang, q. Wang, k. Ren, and w. Lou, "privacy-preserving public auditing for data storage security in cloud computing," in proc. Ieee infocom, mar. 2010, pp. 1–9.
[29] C. Wang, k. Ren, and j. Wang, "secure and practical outsourcing of linear programming in cloud computing," in proc. Ieee infocom, apr. 2011, pp. 820– 828
[30] c.wang, n.cao, j.li, k.ren, and w.lou, "secure ranked keyword search over encrypted cloud data," in proc. Ieee 30th icdcs, jun. 2010, pp. 253 262.
[31] Y. Liu, j. Han, and j. Wang, "rumor riding: anonymizing unstructured peer-to-peer systems," ieee trans. Parallel distrib. Syst., vol. 22, no. 3, pp. 464–475, mar. 2011
[32] Tor: anonymized network. [online]. Available: https://www.torproject.org/, accessed 2014
[33] A. Shamir, "how to share a secret," commun. Acm, vol. 22, no. 11, pp. 612–613, 1979
[34] M. Naor and b. Pinkas, "oblivious transfer and polynomial evaluation," in proc. 31st stoc, 1999, pp. 245–254.
[35] S. Even, o. Goldreich, and a. Lempel, "a randomized protocol for signing contracts," commun. Acm, vol. 28, no. 6, pp. 637–647, 1985.
[36] W.-g. Tzeng, "efficient 1-out-of-n oblivious transfer schemes with universally usable parameters," ieee trans. Comput., vol. 53, no. 2, pp. 232–240, feb. 2004.
[37] Ciphertext-policy attribute-based encryption toolkit. [online]. Available: http://acsc.csl.sri.com/cpabe/, accessed 2014.
[38] W. Ren, k. Ren, w. Lou, and y. Zhang, "efficient user revocation for privacy-aware pki," in proc. Icst, 2008, art. Id 11.
[39] M. Li, s. Yu, y. Zheng, k. Ren, and w. Lou, "scalable and secure sharing of personal health records in cloud computing using attributebased encryption," ieee trans. Parallel distrib. Syst., vol. 24, no. 1, pp. 131–143, jan. 2013.
[40] Taeho jung, xiang-yang li, senior member, ieee, zhiguo wan, and meng wan, member, ieee " control cloud data access privilege and anonymity with fully anonymous attribute-based encryption " ieee transactions on information forensics and security, vol. 10, no. 1, january 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY