International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 08 | August - 2022 Impact Factor: 7.185 ISSN: 2582-3930

An Enhanced and Reliable Cloud Trust Protection Model for Privacy Data

Y. Ujwal kumar , S. Siva krishna, P. Sai mouli
ujwalyallamraju16@gmail.com sanagalasivakrishna@gmail.com mouliroyal764@gmail.com
UG Student ,Department of CSE, Narayana Engineering College, Gudur, Nellore,AP 524101

Mr. P. k. Venkateswar Lal
venkateswarlal@gmail.com
Associate Professor Department of CSE, Narayana Engineering College, Gudur, Nellore,AP 524101

The vulnerability of Cloud Computing Systems (CCSs) to Advanced Persistent Threats (APTs) is a significant concern to government and industry. We present a cloud architecture reference model that incorporates a wide range of security controls and best practices,and a cloud security assessment model – Cloud-Trust – that estimates high level security metrics to quantify the degree of confidentiality and integrity offered by a CCS or cloud service provider (CSP). Cloud-Trust is used to assess the security level of four multi- tenant IaaS cloud rchitectures equipped with alternative cloud security controls and to show the probability of CCS penetration (high value data compromise) is high if a minimal set of security controls are implemented. CCS penetration probability drops substantially if a cloud defense in depth security architecture is adopted that protects virtual machine (VM) images at rest, strengthens CSP an cloud tenant system administrator access controls, and which employs other network security controls to minimize cloud network surveillance and discovery of live VMs.
Keywords: - Cloud Computing, Trust, Trust Management, Trust Models, Privacy, Trust metric, enables CSPs to start, stop, move, and restart

INTRODUCTION: - The flexibility and scalability of CCSs can offer significant benefits to government and private industry. However, it can be difficult to transition legacy software to the cloud. Concerns have also been raised as to whether cloud users can trust CSPs to protect cloud tenant data and whether CCSs can prevent the unauthorized disclosure of sensitive or private information. The literature is rife with studies of CCS security vulnerabilities that can be exploited by APTs Virtualization, the basis for most CCSs, computing workloads on demand. VMs run on computing hardware that may be shared by cloud tenants. This enables flexibility and elasticity, but introduces security concerns. The security statusof a CCS depends on many factors, including security applications running on the system, the hypervisor (HV) and associated protection measures, the design patterns used to isolate the control plane from cloud tenants, the level of protection provided by the CSP to cloud tenant user data and VM images, as well as other factors. These concerns raise questions. Can the overall security status of a CCS or a CSP offering be assessed using a framework that addresses the unique vulnerabilities of CCSs and can such assessments be applied to alternative CCS architectures and CSP offerings in an unbiasedway? The federal government has issued security controls that CSPs must implement to obtain FEDRAMP CCS security certification that are based on National Institute of Standards and Technology (NIST) cloud security guidelines. However, these do not provide high-level decision- makers with an overall assessment ofCCS security status or the degree of confidentiality and integrity offered by specific cloud architectures. The main contributions of this paper are to develop a CCS reference architecture and a cloud security assessment model – Cloud-Trust – that provides quantitative high-levelsecurity assessments of IaaS CCSs and CSPs. Cloud-Trust can assess the relative level of security offered by alternative CSPs or cloud architectures. Cloud tenants can use it to make decisions on which CSP security options or cloud security features to implement[1][2][3]. We illustrate the use of Cloud-Trust by applying it to the casewhere the cloud tenant is a U.S. government agency and examine

how well four alternative CCS architectures protect U.S. government data. Cloud-Trust is based on CCS unique attack paths that cover the essential elements of an IaaS cloud architecture. It is based on a Bayesian network model of the CCS, the class of APT attack paths spanning the CCS attack space, and the APT attack steps required to implement each attack path. It provides two key high-level security metrics to summarize CCS security status quantitatively: • Probability an APT can access high value data Probability the APT is detected by cloud tenant or CCS security monitoring systems The first security metric estimates whether high value data (designated as "Gold" data in this paper) is likely to be compromised or erased from the CCS. The second metric assesses whether the CSP provides cloud tenants sufficient CCS network monitoring, file access, and situation awareness data to detect intrusions into a tenant's cloud network, and whether the tenant's security and monitoring systems contribute to the intrusion detection. This paper is organized as follows. Section 2 discusses trust zones. Section 3 presents a cloud reference model and cloud security control features[11]. Section 4 describes CCS unique attack paths and vulnerabilities that can be exploited by APTs. Section 5 describes Cloud-Trust. The final section provides Cloud-Trust results for four alternative CSP offerings[12][13].

RELATED WORK: -

The real fact that Attribute Based Encryption has demonstrated its benefits, client renouncement and Attribute denial is the essential concerns. The denial issue is much progressively troublesome particularly in Cipher Text Policy-Attribute Based Encryption plans, in light of the fact that each Attribute is shared by numerous clients. This implies repudiation for any property or any single client may influence different clients in the framework. As of late, some work has been proposed to equipment this issue in productive manners. Productive renouncement, which is additionally appropriate for Key Policy- Attribute Based Encryption All things considered, it isn't evident whether their plan is appropriate forCipher Text Policy-Attribute Based Encryption. Characteristic based information offering plan to quality denial capacity.

Attribute Based Encryption Over View:-

This plan was demonstrated that it's a secure data against picked original data leaked in light of data assumption. Be that as it may,the length of secure data and client's secret key are relative to the quantity of qualities in the characteristic universe. In the key age, encryption and decoding stages, calculation includes all properties in theAttribute universe. Subsequently, it is costly in correspondence and calculation cost for clients. It supports technique to perform client renouncement activity byjoining Cipher Text Policy-Attribute Based Encryption with re-encryption. In their plan, every client has a place with a gathering and holds a gathering secret key gave by the gathering. Be that as it may, their plan doesn't avoid agreement physically attack performed by revoked clients collaborating with existing clients. The explanation is that every client's gathering secret key is same in a similar gathering. The properties of the renounced clients can be utilized by the client in a similar gathering without the predetermined attributes. Moreover, we bring up that there is a similar security chance in the plans through applying Attribute Based Encryption plans to distributed storage administrations, we canboth guarantee the security of put away information and accomplish fine-grained information access control. Tragically, Attribute Based Encryption plan requires high calculation overhead during performing encryption and unscrambling tasks. This deformity turns out to be increasingly extreme for lightweight devices because of their compelled registering assets. To diminish the calculation cost for asset compelled devices, some cryptographic tasks with high computational burden were re-

appropriated to cloud specialist organizations intermediary re-encryption with languid re-encryption procedure, structured a Key Policy- Attribute Based Encryption conspire with fine-grained information access control. This plan necessitates that the root hub in the entrance tree is an AND door and one kid is a leaf hub which is related with the fake Attribute. The fake credit is required to be incorporated into each datum report's Attribute set and will never be refreshed. In their plan, cloud specialist organization stores the entire private key segments for user's private key apart from the one relating to the spurious quality Be that as itmay, cloud specialist organization doesn't gain proficiency with the plaintext for any information record. There are few entities while encrypting data before uploading inside online cloud server.

Symbol	Description
TA	Trusted Authority
GM	Trusted Group Manager
DO	Data Owner
DU	Data User
CSS	Cloud Storage Server
E-CSP	Encryption-Cloud Service Provider
D-CSP	Decryption-Cloud Service Provider

Table 2.1 Explanation of Symbols

The secure data Cipher Text Policy-Attribute Based Encryption conspire with client denial; we expect that a client's private key incorporates two sections. One is related with his approved properties and the other one is related with the gathering which he has a place with. At the point when at least one data receiver leave the gathering, GM updates gathering key pair and updates private keys for existing clients. To disavow their entrance capacity to the put away information, GM likewise applies for re-encryption tasks from CSS. A work process of all calculations is portrayed in below figure. A Cipher Text Policy-Attribute Based Encryption plot with client disavowal comprises of the accompanying proper calculations.

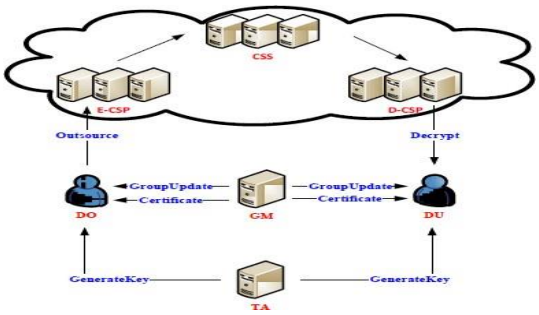

Figure 2.1 Architecture of Storage System

Performance Evaluation

Attribute Based Encryption Storage System buildon Cipher Text Policy-Attribute Based Encryption scheme. Let's the parameters $|pars|$, $|msk|$, $|CT|$, $|L|$, $|T|$, $|SK|$, $|A|$ be the sizes of the parameters open parameter, ace private key, figure message, the attribute, the attached data , the decoding key and the entrance structure, separately . Connote l by the quantity of properties in a passageway structure, and k by the size of a credit set ascribed to a customer's confirmations. Table 1 takes a gander at the limit multifaceted nature of our structure. Clearly our structure is capable as far as the introduced accumulating overhead, which incorporates the essential Cipher Text Policy- Attribute Based Encryption parts to the systemopen parameter and 3 segments to the figure content set away by the insecure cloud server, with an additional private cloud taking care of 3 segments. Allow l is for the number of attributes displayed in a passageway structure, and k is the size of a characteristic set related with the private key. Show y by the amount of existing names set away by the private cloud. The Table shows the quantity of mathematical exponent and paring exercises in our storing system. For example, it requires everything considered k + 2 exponential exercises what's more, 3k + 1 paring assignments to translate figure content. The above Table

considers the computer related costs realized at the Data supplier the cloud, and the customer for one record storing our structure. It isn'tinconvenient to see that the computational essential for the customer in our structure is twice that in the covered up Cipher Text Policy- Attribute Based Encryption Regarding the data provider, it requires 4 extra mathematical exponent assignments came about in view of the tag, name, affirmation and unauthorized access key despite the computational Cost of the concealed arrangement message in missing the mark on the capacity of secure de duplication. With respect to private cloud, our course of action takes 5 + (6l + 2) exponential exercises and 2y mixing exercises, among which 5 exponential assignments Are used to check the authenticity of the proof, 6l+2 exponential exercises are related tothe figure content recuperation if vitaladditionally, 2y mixing exercises are resolved to check paying little heed to whether the normal text concealed in the redistributing sales has existed in the open cloud.

Variable attribute based Encryption:-

It shows cryptographic unrefined called versatile Cipher text Policy-ATTRIBUTE BASED ENCRYPTION, where a semi-accepted delegate is exhibited into the setting of Cipher Text Policy-Attribute Based Encryption. The middle person, given a system wide unauthorized access key, can change any figure message under one access methodology into figure writings of the comparable plaintext under some different access methodologies without adjusting any data related information about the plaintext during the technique of progress. Regardless, this strategy for using a lone unauthorized access key for all figure writings is extremely perilous, since if the single key is exchanged off, the security for the system will be totally broken. A badly arranged customer using the dealt unauthorized access key can recuperate a figure content into a passage Basic Model that? His/her characteristics satisfy, and thusly he/she can get the plaintext not expected for him/her. Also, the unauthorized access key is created by the AA who starting at now controls the unscrambling keys in the structure, so it is appealing to decrease its ability in controlling the encryption. Our framework is facilitated with the ultimate objective that each unauthorized access key must be used to change its contrasting figure content. As such, even in the end, a unauthorized access key is included; the mischief is limited to one message. At a raised level, our technique conveys another way to deal with creates adaptable CIPHER TEXT POLICY-ATTRIBUTE
BASED ENCRYPTION outline works from a substitute viewpoint.

II. Related Work: -

Cipher Text Policy-Attribute Based Encryption Schema with Verifiable Secure Decryption

We at first propose another Cipher Text Policy-Attribute Based Encryption plan utilizing Waters' Cipher Text Policy-Attribute Based Encryption plots, which is shown to be explicitly CPA-secure. By then, considering thearrangement, we propose a Cipher Text Policy- Attribute Based Encryption plot with re-appropriated unscrambling and exhibit that it is explicitly CPA-secure and undeniable in the standard model. Starting late, the first Cipher Text Policy-Attribute Based Encryption plan that practiced full security was proposed. Since the central structure of the Cipher Text Policy-Attribute Based Encryption. We use, one can change our advancement frameworks to the Cipher Text Policy-Attribute Based Encryption plan proposed to achieve totally secure Cipher Text Policy-Attribute Based Encryption contrive with verifiable redistributed unscrambling in the standard model.

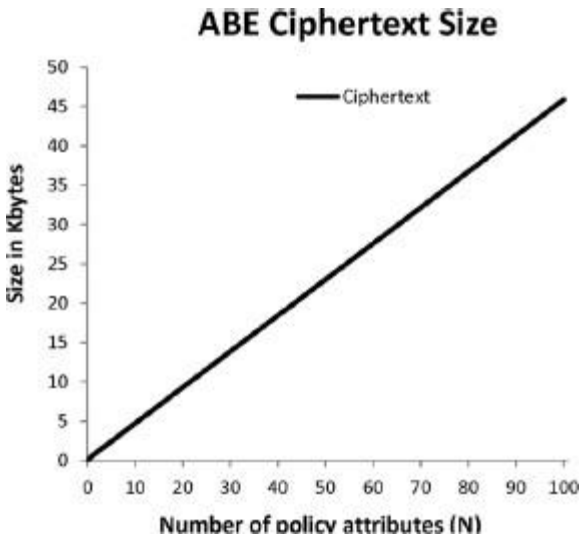

Figure 2.3.1(a) Calculating cipher text sizeIn a Cipher Text Policy-Attribute Based Encryption scheme, the complexity of cipher text arrangement impacts both the decryption time and the cipher text size. We create cipher text strategies in the form of (A_1,A_2……A_N) circumstance over the approach), where A_i is an Attribute.

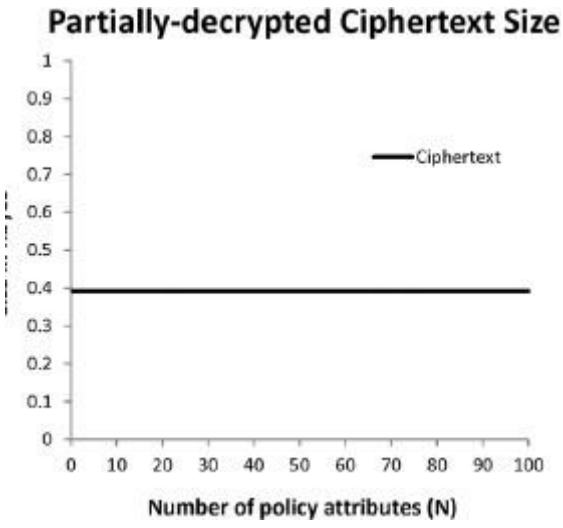

Figure 2.3.1(b) Partially Decrypted Cipher textsize
The above Diagram represents the entire System will be depends upon the security if the secure decryption fails immediately the encrypted text doesn't support to decrypt properly.

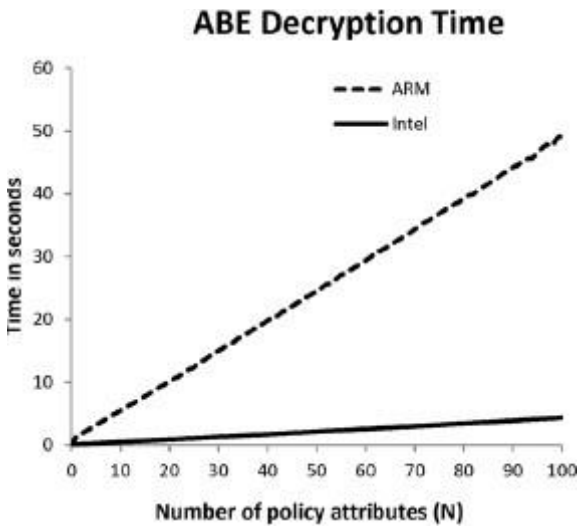

Figure 2.3.1 (C) Cipher Text Policy-Attribute Based Encryption Decryption Time
It shows the result of completely decrypted text time and the functions only allows to user after generated keys.

Cipher Text Policy-Attribute Based Encryption System with OutsourcedDecryption

Consider a cloud based electronic therapeutic record structure in which patients' helpful records are guaranteed using Cipher Text Policy-Attribute Based Encryption plans with redistributed unraveling and are taken care of in the cloud. In order to beneficially get to patients' remedial Records on her mobile phone, a pro delivers and delegates a change key to a mediator in the cloud for re-appropriated translating; given a changed figure content from the middle person, the pro can scrutinize a patient's restorative record by just playing out a clear advance of count. If verification of the correctness of the change is not guaranteed, in any case, the structure can continueto function with two problems:

1) With the ultimate goal of saving hiring costs, the mediator may reinstate a medical record hitherto changed by a comparable authority.

2) Due to system failure or malicious ambush, the intermediary could send the useful history of another patient or a file of the correct structure in any case, transmitting erroneous information.

The result of treating the patient subject to misinformation could be extreme or, on the other hand, even disastrous. The above observation leads us to inspect attribute-based encryption of ciphertext policies with apparent reappropriateddecryption in this document. We note that a Ciphertext Policy Attribute-Based Encryption is conceived with a secure redistributed decryption that generally does not guarantee a certain nature.

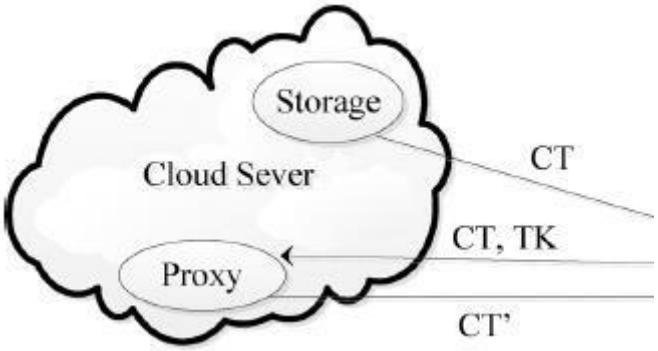

Figure 2.3.2 Cipher Text Policy-Attribute Based Encryption System with outsourced decryption

Intermediary Re Encryption:

In Cipher Text Policy-Attribute Based Encryption with redistributed unscrambling, a customer outfits the cloud with a change key that allows the cloud to unravel a Cipher Text Policy-Attribute Based Encryption figure message on message into an essential figure message on the comparable, without grabbing anything about. This is reminiscent of the possibility of middle person re encryption. Delegate re encryption allows a middle person, using are encryption key, to change an encryption of under Alice's open key into an encryption of the identical under Bob's open key without the mediator grabbing anything about the encoded Message. We underscore that in the model of go-between encryption; proof of the mediator's change can't be cultivated. This can be immediately explained as seeks after. A mediator could replace the encryption of under Alice's open key with the encryption of another message under Alice's open key and after that usage its re encryption key to change the last into an encryption of under Bob's open key. Plainly, without participation with Alice, Bob can't perceive this threatening behavior of the middle person.

Cipher Text Policy- Attribute Based Encryption with outsourced Decryption

In the first model characterized in, a Cipher Text Policy-Attribute Based Encryption conspire with re-appropriated decoding comprises of five calculations: furthermore, . A trusted gathering utilizes the calculation to produce the open parameters also, an ace mystery key, and uses to produce a private key and a change key for a client. Taking as input the change key given by a client and a cipher text, the cloud can utilize the calculation to change the cipher text into a straightforward cipher text if the client's quality fulfills the entrance structure related with the cipher text; at that point the client utilizes the calculation to recuperate the plaintext from the changed cipher text, the contribution to the calculation incorporates just the private key to develop a Cipher Text Policy-Attribute Based Encryption Plot with evident redistributed unscrambling under the definition.This can be clarified as pursues. A pernicious cloud could supplant the cipher text it assumes to change with a cipher text of an alternate message, and after that change the last into a straightforward cipher text utilizing its change key. Clearly, the client can't recognize this vindictive conduct of the cloud since the contribution to the calculation doesn't incorporate the first cipher text required to be changed. Inrequest to accomplish certainty, we have to adjust the model of Cipher Text Policy-Attribute Based Encryption with re-appropriated decoding. We now officially depict our new model. A Cipher Text Policy-Attribute Based Encryption conspires with re-appropriated unscrambling comprises of the accompanying sevencalculations.

Verifiable Delegation Technique Verifiable Delegation (VD) is utilized to ensure approved clients from being misdirected during the assignment. The information proprietor scrambles his message M under get to arrangement f, at that point registers the

supplement circuit if, which yields the contrary piece of the yield of f, and scrambles an arbitrary component R of the equivalent length to M under the arrangement. The clients can at that point redistribute their unpredictable access control approach choice what's more, part procedure of unscrambling to the cloud. Such expanded encryption guarantees that the clients can get either the message M or the irregular component R, which maintains a strategic distance from the situation when the cloud server misdirects the clients that they are not fulfilled to the entrance strategy, be that as it may, they meet the entrance arrangement really. In Cipher Text Policy-Attribute Based Encryption we utilize a half breed variation for two reasons: one is that the circuit Cipher Text Policy-Attribute Based Encryption is a piece encryption, and the other is that the validation of Based Encryption for circuits it makes up the key exemplification component part, and a symmetric encryption in addition to the encode make up the verified encryption component (AC) part. Each KEM encodes an irregular bunch component and afterward maps it by means of key determination capacities into a symmetric encryption key and a once checked key vk. At that point the irregular encryption key dk is utilized to encode the message of any length. vk and the information proprietor's ID are utilized to check the Macintosh of the cipher text. Just when the server portion not produce the first cipher text and react a right halfway unscrambled cipher text, the client might appropriately approve the MAC. For usage, the ongoing work on multi linear maps over the numbers is applied to reproduce conspire in the GMP library in VC 6.0. Despite the fact that the activity time for the matching in the multi linear guide is considerably more than the one in the bilinear guide, we could accomplish the most grounded general circuits get to approach up to now. Moreover, by utilizing undeniable assignment, the activity time for the client is short and autonomous of the unpredictability of the circuit. For the security, we demonstrate that the IND-CPA secure KEM consolidates with the IND-CCA secure verified (symmetric) encryption plan yields our IND-CPA secure mixture VD-CP Cipher Text Policy-Attribute Based Encryption plot.

Security Model

In our passage control system, the cloud is believed to be "straightforward however inquisitive", which resembles by far most of the related compositions in the subject of cloud secureamassing: On one hand, it offers reliable accumulating organization and viably executes every computation key various components; On the other hand, it may endeavor to increment unapproved information for its very own advantages.. CA is responsible for key course and time token disseminating. We acknowledge that a dangerous customer may endeavor to unscramble the figure content to gain UN affirmed data unquestionably, consolidating plotting with different customers. The proposed TAFC can comprehend a fine-grained and coordinated discharge get to control system: Only a customer with satisfied property set can get to the data after the allocate time.

III. Literature Survey: -

1) A technique for computer detection and correction of spelling errors AUTHORS: F. J. Damerau

The method described assumes that a word which cannot be found in a dictionary has at most one error, which might be a wrong, missing or extra letter or a single transposition. The unidentified input word is compared to the dictionary again, testing each time to see if the words match—assuming one of these errors occurred. During a test run on garbled text, correct identifications were made for over 95 percent of these error types.

2) LIBSVM: A library for support vector machines

AUTHORS: C.-C. Chang and C.-J. Lin

LIBSVM is a library for Support Vector Machines (SVMs). We have been actively developing this package since the year 2000. The goal is to help users to easily apply SVM to their applications. LIBSVM has gained wide popularity in machine learning and many other areas. In this article, we present all implementation details of LIBSVM. Issues such as solving SVM optimization problems theoretical convergence multiclass classification probability estimates and parameter selection are discussed in detail.

3) Beyond blacklists: Learning to detect malicious Web sites from suspicious URLs

AUTHORS: J. Ma, L. K. Saul, S. Savage, and G. M. Voelker

Malicious Web sites are a cornerstone of Internet criminal activities. As a result, there has been broad interest in developing systems to prevent the end user from visiting such sites. In this paper, we describe an approach to this problem based on automated URL classification, using statistical methods malicious Web site URLs. These methods are able to learn highly predictive models by extracting and automatically analyzing tens of thousands of features potentially indicative of suspicious URLs. The resulting classifiers obtain 95-99% accuracy, detecting large numbers of malicious Web sites from their URLs, with only modest false positives.

4) Design and evaluation of a real-time URL spam filtering service

AUTHORS: K. Thomas, C. Grier, J. Ma, V.Paxson, and D. Song

On the heels of the widespread adoption of web services like social media and URL shorteners, scams, phishing, and malware have become common threats. Despite extensive research, email-based spam filtering techniques generally fail to protect other web services. To better address this need, we are introducing Monarch, a real-time system that tracks URLs as they are submitted to web services and determines if the URLs are leading to spam. We assess the viability of Monarch and the fundamental challenges that arise due to the diversity of web service spam. We show that Monarch can provide accurate real-time protection, but that the underlying characteristics of spam are not generalized across web services. In particular, we found that email targeted at spam differed qualitatively significantly from spam campaigns targeted at Twitter. We explore the distinctions between email and Twitter spam, including abuse of redirection services and public web hosting. Finally, we demonstrated Monarch's scalability, showing that our system could protecta service like Twitter, which needs to process 15 million URLs per day, for just under $800 per day.

5) Detecting spammers on social networks

AUTHORS: G. Stringhini, C. Kruegel, and G. Social networks have become a popular way for users to meet and interact online. Users spend a significant amount of time on popular social networking platforms (such as Facebook, MySpace or Twitter), storing and sharing a large amount of personal information. This information,in addition to the possibility of contacting thousands of users, also attracts the interest of cybercriminals. For example, cybercriminals can exploit implicit trust relationships between usersto lure victims to malicious websites. As another example, cybercriminals can find valuable personal information for identity theft or to drive targeted spam campaigns. In this document, we analyze the extent to which spam has enteredsocial networks. More precisely, we look at how spammers targeting social networking sites operate. To collect the data on spam activity, we created a large and diverse set of "honey profiles" on three major social networking sites andrecorded the type of contacts and messages they received. We then analyze the collected data and identify abnormal behavior of users who contacted our profiles. From the analysis of thisbehavior, we develop techniques to detect spammers in social networks and we add their messages in large spam campaigns. Our results show that it is possible to automatically identify accounts used by spammers, and our analysis was used for takedown efforts in a real-world social network. More precisely, during this study, we

collaborated with Twitter and successfully detected and removed 15,857 spam profiles.

Proposed Algorithm: -

Trapdoor creates encryption strategies that use cipher text policy attributes when the software uploads and saves the time if the key is not correctly identified as an incorrect user. With the arrangement A, a trapdoor key is given to the private cloud that is produced by an information supplier alongside the figure material c. For Strategy A and other Figure C material a new A0 entrance strategy without understanding the fundamental message M can be used for the private cloud to turn over the Figure c content. It helps the private cloud to retrieve figural material for the corresponding secret document by means of an entry technique, when two suppliers of information pass two figures relating to a similar record, but under different access arrangements An and A0. The Trapdoor Schussed and the figure message are located in the general public cloud rather than the previous one. The key test for secure de-duplication is to insure that a legitimately generated message is not misrepresented substituted by a fake copy attack. In such an attack, the malicious customer will block a re- appropriation request and alter the figure content afterwards.

IV. Conclusion: -

In this research the storage and security gives more importance with relevant to secret key and generated trapdoor, to maintain resist online attack, we embed a certificate into the user's private key. So that malicious users and the revoked users do not have the ability to generate a valid private key. The results of our experiment show that our scheme is efficient for resource constrained generators. Securing data outsourced to the cloud against an adversary which has access to the encryption key. Encryption key, and all but two cipher text blocks, each and every block assigned to one key that is public or else private key. The adversary would need to acquire the encryption key, and to compromise all servers.Finally, we showed how attribute based storage be practically integrated within existing dispersed storage systems. Our proposed scheme provides a possible way to fight against immoral interference with the right of privacy. We hope more schemes can be created to protect cloud. Proposed techniques failed to explain the online guessing attacks.

V.REFERENCES

I. Ali, M., Dhamotharan, R., Khan, E., Khan, S.U., Vasilakos, A.V., Li, K., Zomaya, A.Y. (2014) SeDaSC: Secure Data Sharing in Clouds, IEEE Syst. J.(2015).

II. Ali, M., Dhamotharan, R., Khan, E., Khan, S.U., Vasilakos, A.V., Li, K., Zomaya, A.Y. (2017) 'SeDaSC: Secure Data Sharing in Clouds', IEEE Systems Journal, 11(2), 395–404.

III. Androulaki, E., Soriente, C., Malisa, L., Capkun, S. (2014) 'Enforcing Location and Time-Based Access Control on Cloud-Stored Data', in 2014 IEEE 34th International Conference on Distributed Computing Systems, Presented at the 2014 IEEE 34th International Conference on Distributed Computing Systems, 637–648.

IV. Arora, R., Parashar, A. (2013) 'Secure User Data in Cloud Computing Using Encryption Algorithms'.

V. Arora, R., Parashar, A., Transforming, C.C.I. (2013) 'Secure user data in cloud computing using encryption algorithms', International journal of engineering research and applications, 3(4), 1922–1926.

VI. Bethencourt, J., Sahai, A., Waters, B. (2007) 'Ciphertext-policy attribute- based encryption', in 2007 IEEE Symposium on Security and Privacy (SP'07), IEEE, 321–334.

VII. Cai, K., Hong, C., Zhang, M., Feng, D., Lv, Z. (2013) 'A secure conjunctive keywords search over encrypted cloud data against inclusion-relation attack', in 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, IEEE, 339–346.

VIII. Chen, J., Ma, H. (2014) 'Efficient decentralized attribute-based access control for cloud storage with user

revocation', in 2014 IEEE International Conference on Communications (ICC), IEEE, 3782– 3787.

IX. Cui, H., Deng, R.H., Li, Y., Wu, G. (2019) 'Attribute-Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud', IEEE Transactions on Big Data, 5(3), 330–342.

X. Fan, K., Tian, Q., Wang, J., Li, H., Yang, Y. (2017) 'Privacy protection based access control scheme in cloud-based services', China Communications, 14(1), 61–71.

Ferreira, B., Rodrigues, J., Leitão, J., Domingos, H. (2019) 'Practical Privacy-Preserving Content-Based Retrieval.

[11]Mandava Geetha Bhargava, Modugula TS Srinivasa Reddy, Shaik Shahbaz, P Venkateswara Rao, V Sucharita Potential of big data analytics in bio-medical and health care arena: An exploratory study, Global Journal of Computer Science and Technology 2017/8/5

[12]V.Sucharita, P.Ravinder Rao,"A Framework to Automate Cloud based Service Attacks Detection and Prevention"(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 2, 2019

[13]Kollu, A., Sucharita, V. (2018). Energy-Aware Multi-objective Differential Evolution in Cloud Computing. In: Dash, S., Das, S., Panigrahi, B. (eds) International Conference on Intelligent Computing and Applications. Advances in Intelligent Systems and Computing, vol 632. Springer,Singapore. https://doi.org/10.1007/978-981-10-5520-1_40