As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 7(10): 40-47, 2021

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0710006
Available online at: http://www.ijmtst.com/vol7issue10.html

An Enhanced Technique to discover web data extraction and Data mining in Multi Cloud Server

Dadi Madhu SivaRama Krishna[1] | S.Suryanarayana Raju[2] | Ajay Dilip Kumar Marapatla[3]

[1]M.Tech Student, Department of CSE, SRKR Engineering College, Bhimavaram, India.
[2]Department of CSE, SRKR Engineering College, Bhimavaram, India.
[3]Department of CSE, SRKR Engineering College, Bhimavaram, India.

To Cite this Article
Dadi Madhu SivaRama Krishna, S.Suryanarayana Raju and Ajay Dilip Kumar Marapatla. An Enhanced Technique to discover web data extraction and Data mining in Multi Cloud Server. *International Journal for Modern Trends in Science and Technology* 2021, *7*, pp. 40-47. https://doi.org/10.46501/IJMTST0710006

Article Info
Received: 03 September 2021; Accepted: 28 September 2021; Published: 30 September 2021

ABSTRACT

Data mining is a critical stage in the Knowledge Discovery process acquire from databases (KDD), thus a new approach that's can joint with online data process of extraction, which serves as data gathering from the global network (web), and data mining techniques is required.The primary contribution of this study is the proposal of a system for collecting categorical online data on several cloud servers while ensuring data security and integrity for consumers. The algorithms' effectiveness employed inside our technique is illustrated using clustered sections of the data that should be encrypted inside the cloud server combining the three clustering measurements precision, recall, and accuracy. We proposed KeyGen algorithm to maintain data security by using cryptographic concepts with respective ABE (attribute-based encryption) and cypher text policy (cypher text policy) are two types of attribute-based encryption (CP-ABE).

KEYWORDS: Cryptography, CP-ABE, Cloud Server, KDD.

I. INTRODUCTION

Client renunciation and attribute denial are the primary issues, despite the fact that Attribute Based Encryption has proven to be beneficial. As a result of the fact that each Attribute is shared by several clients, the denial issue is becoming increasingly problematic, particularly in Encryption of Cipher Text Using Policy Attributes designs. 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 equipmentthis 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 for Encryption of Cipher Text Using Policy Attributes. Characteristic based information offering plan to quality denial capacity.

II. LITERATURE SURVEY

F. J. Damerau et.al. [1] The approach implies that there is only one error in a term that cannot be found in a dictionary, as an example, a single transposition or an incorrect, missing, or additional letter. If one of these mistakes happened, the unrecognised input word is checked against the dictionary once again, checking to see whether the words are the same each time during a

trial run with jumbled text, almost 95 percent of these problem categories were correctly identified.

C.-C. Chang and C.J. Lin [2] proposed LIBSVM is a Support Vector Machines library (SVMs). Since the year 2000, they have been working on this package. The goal is to make applying SVM to apps as straightforward as possible for users. LIBSVM is a programming language that is widely used in machine learning and a number of other disciplines. They detailed the LIBSVM implementation in this paper. We go through topics like addressing SVM in-depth discussion of optimization issues, theoretical convergence, multiclass classification probability estimates, and parameter selection.

J. Ma, L. K. Saul, S. Savage, and G. M. Voelker [3] Malicious Web sites are a key component of online criminal activity. As a result, there has been a significant amount of interest. Building mechanisms to keep end users away from similar websites. In this article, they were provided an automated URL classification solution to this challenge, which employ statistical methods to identify [17] the telltale lexical and host-based features of fraudulent Web site URLs. By automatically collecting and assessing tens of thousands of indicators that might indicate dubious URLs, these techniques are able to create highly predictive models. The classifiers that result achieve 95-99 percent accuracy, with just small false positives, recognising a large number of hazardous Web sites from their URLs.

K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song [4] proposed Scams, phishing, and malware have grown commonplace as a result of increased use of web services like social networks and URL shorteners. Despitesignificant study, email-based spam filtering solutions fail to adequately safeguard different types of web services Monarch is a real-time system that examines URLs as they are submitted to internet services and determines if they lead to spam.We assess Monarch's viability and the basic problems it faces as a result of the wide variety of online service spam. Monarch [19] has shown that it is capable of providing accurate, real-time security, but that spam's fundamental features do not apply to all online services. We discovered that spam targeting email differed significantly from spam operations targeting Twitter in terms of quality. They investigated the distinctions between spam sent via email and spam sent via Twitter, as well as the abuse of public web hosting and redirection services. Finally, they demonstrated Monarch's scalability, proving that for less than $800 per day, our system could protect a service like Twitter, which handles 15 million URLs each day.

G. Stringhini, C. Kruegel proposed Users are increasingly meeting and interacting online through social networking sites. Users spend a lot of time on major social networking sites like Facebook, Twitter and Myspace are all save and share a great deal of personal information.. Cybercriminals are interested in this information since it gives them the ability to contact thousands of users. Cybercriminals might, for example, take advantage of consumers' implicit trust connections to entice them to harmful websites. Personal information, for example, may be useful to hackers who use it to commit identity theft or run targeted spam operations. They investigated the extent to which spam has infiltrated social networks in this research. They look at how spammers use social networking sites as a target function in more detail. They built a wide and diversified set of "honey-profiles" to collect statistics about spamming behaviour on three major social networking sites, and documented the kind of contacts and messages they got. The acquired data was subsequently examined, and unusual conduct of people who contacted our profiles was discovered [18]. Then created algorithms to detect spammers in social networks based on this data, and they consolidated their communications into massive spam campaigns. Their findings demonstrated that spammers' accounts can be automatically identified, and their findings were used to shut down operations in a real-life social network [21]. More specifically, they cooperated with Twitter throughout this investigation and properly identified and removed 15,857 spam profiles.

III. RELATED WORK

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

We first present a Encryption of Cipher Text Using Policy Attributes plan that is expressly CPA-secure, based on Waters' Encryption of Cipher Text Using Policy Attributes [6] plots. By then, we've proposed a

Encryption of Cipher Text Using Policy Attributes scheme with re-appropriated unscrambling and demonstrated that it's explicitly CPA-secure[23] and irrefutable in the traditional model,. The first Encryption of Cipher Text Using Policy Attributes scheme was proposed late. Since the Encryption of Cipher Text Using Policy Attributes basic structure. In the traditional model,, we utilise, and we may convert our advancement frameworks to the Encryption of Cipher Text Using Policy Attributes plan presented to create completely safe Encryption of Cipher Text Using Policy Attributes contrivance with verifiable redistributed unscrambling.

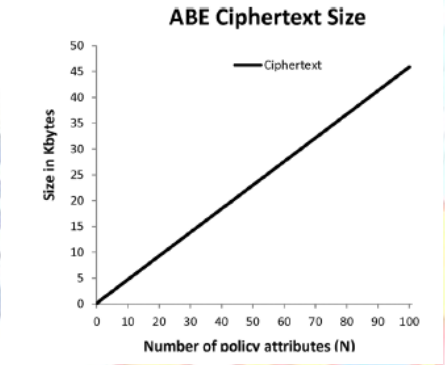


Figure 2.3.1(a) calculating the size of encrypted text

The complexity of the cypher text arrangement affects both the decryption time and the cypher text size in aEncryption of Cipher Text Using Policy Attributes scheme [16]. We create cipher text strategies in the form of (A1,A2……AN) circumstance over the approach), where Ai is an Attribute.

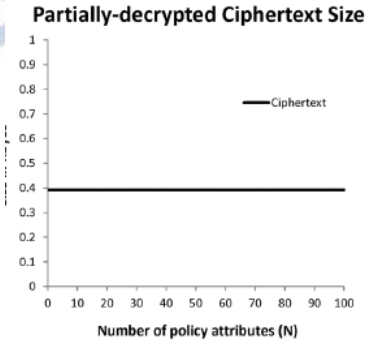


Figure 2.3.1(b) Partially Decrypted Cipher text size

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.

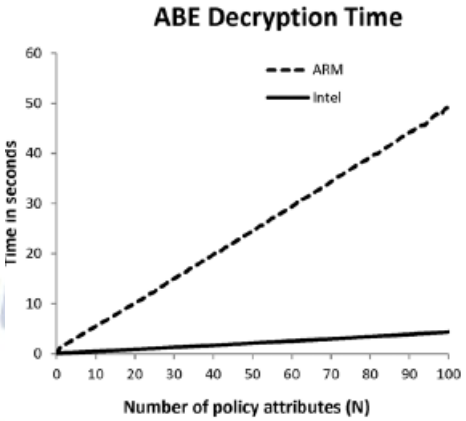


Figure 2.3.1 (C) Encryption of Cipher Text Using Policy Attributes Decryption Time

It shows the result of completely decrypted text time and the functions only allows to user after generated keys.

Outsourced Decryption System for Encryption of Cipher Text Using Policy Attributes

Consider a cloud-based electronic therapeutic record structure in which patients' useful records are protected in the cloud utilising Encryption of Cipher Text Using Policy Attributes schemes with redistributed unravelling [2]. A professional delivers and delegated a change key to a mediator in the cloud for re-appropriated translating in order to benefit ably get to patients' remedial Records on her mobile phone; given a changed figure content from the middle person, the pro can scrutinise a patient's restorative record by simply playing out a clear advance of count [9]. If no check of the rightness of the change is guaranteed, in any case, the structure may continue running into the going with two issues:

1) With the ultimate objective of saving enlisting cost, the mediator could re-establish a medicinal record changed heretofore for a comparable authority

2) In the event of a system failure or a malicious ambush, the go-between may provide an useful record of another patient or an archive of the proper structure in any case, passing on incorrect information.

The result of treating the patient subject to off kilter information could be extreme or on the other hand even disastrous. The above observation rouses us to inspect Encryption of Cipher Text Using Policy Attributes with apparent re-appropriated unscrambling in this paper. We highlight that an Encryption of Cipher Text Using

Policy Attributes contrive with secure redistributed unraveling doesn't generally guarantee certain nature For example, the safe Encryption of Cipher Text Using Policy Attributes plans with re-appropriated disentangling.

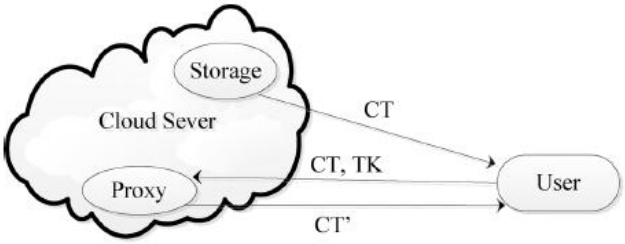


Figure 2.3.2 Encryption of Cipher Text Using Policy Attributes System with outsourced decryption

Intermediary re encryption: In Encryption of Cipher Text Using Policy Attributes with redistributed unscrambling, a customer outfits the cloud with a change key that allows the cloud to unravel aEncryption of Cipher Text Using Policy Attributes figure message on message into an essential figure message on the comparable [7], without grabbing anything about. This is reminiscent of the possibility of middle personre encryption. Delegate re encryption allows a middle party to change an encryption based on Alice's open key to one based on Bob's open key using their encryption key without the mediator gaining access to the encoded Message. We emphasise that proof of the mediator's change cannot be cultivated in the go-between encryption paradigm. This is easily stated as "seeks after." A mediator may replace the encryption of one message under Alice's open key with the encryption of another under Alice's open key, then use its own encryption key to change [3] the last into an encryption of under Bob's open key. Bob can't see the middle person's threatening conduct since he isn't interacting with her.

Attribute-Based Encryption with Outsourced Decryption for Cipher Text Policy

In the first model characterized in, a Encryption of Cipher Text Using Policy Attributes [2] 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 it to generate a client's private key and change key. Using a client-supplied change key and a cypher text as input, the cloud[4] 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 [5] key of the client and the changed cipher text, yet does exclude the first cipher text. As a result of this oversight of the first cipher [7] text, it is preposterous to expect to develop a Encryption of Cipher Text Using Policy Attributes 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[9] 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. In request to accomplish certainty, we have to adjust the model of Encryption of Cipher Text Using Policy Attributes [11] with re-appropriated decoding. We now officially depict our new model. AnEncryption of Cipher Text Using Policy Attributes conspires with re-appropriated unscrambling comprises of the accompanying seven calculations.

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 [6]. under the arrangement, registers the supplement circuit if, which gives the opposite portion of f's yield, and scrambles an arbitrary component R of the corresponding length to M. Clients can then transfer their erratic access control technique choice, as well as part of the unscrambling operation, to the cloud. [8] Such enhanced encryption ensures that clients can get either the message M or the erroneous component R, avoiding the circumstance where the cloud server misdirects clients into believing they are not satisfied with the entrance method when, in reality, they are. In Encryption of Cipher Text Using Policy Attributes we utilize a half breed variation for two reasons:[10] one is

that the circuit Encryption of Cipher Text Using Policy Attributes is a piece encryption, and the other is that the validation of the assigned cipher text ought to be ensured. The cipher text of the half breed VD-CP Encryption of Cipher Text Using Policy Attributes framework is separated into two segments: the Encryption of Cipher Text Using Policy Attributes for circuits it makes up the key exemplification component part, and a symmetric encryptionin addition to the encode make up the verified encryption component (AC) part. Each KEM encodes an irregular bunch component and then translates it into a symmetric encryption key and a once-checked key vk using key determination capabilities. The message of any length is then encoded using the irregular encryption key dk. [12] The Macintosh of the encrypted text is checked using vk and the information owner's ID. The client may approve the MAC if the server fails to deliver the initial cypher text and instead responds with a partly unscrambled cypher text.To recreate conspire in the GMP library in VC 6.0, the continuing work on multi linear maps over integers is used. Despite the fact that the matching activity time in the multi linear guide is significantly longer than in the bilinear guide, we were able to achieve the most grounded general circuits method to date. Furthermore, by employing undeniable assignment, the client's activity time is reduced and is independent of the circuit's unpredictability [11]. In terms of security, we show that combining the IND-CPA secure KEM with the IND-CCA secure verified (symmetric) encryption scheme gives our IND-CPA secure combination.

IV. METHODOLOGY

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 secure amassing: 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. Past the cloud, the whole structure includes one CA, various owners and customers, wherein CA is believed to be totally trust, while customers can be dangerous. 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, [13] 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.

Attribute Based Encryption overview

In light of data assumption, this approach was proven to be a secure data against chosen original data leaked.Regardless, the number of characteristics in the characteristic universe is proportional to the length of secure data and the client's secret key. Calculation encompasses all characteristics during the key age, encryption, and decoding stages in the Attribute universe. As a result, it is costly in terms of correspondence and cost calculation for clients By combining Encryption of Cipher Text Using Policy Attributes with re-encryption, it offers a method for doing client renouncement action. Every customer has a location with a gathering and a gathering secret key given by the gathering, according to their strategy. Regardless, their strategy does not prevent revoked clients from working with current clients to physically challenge the agreementThe reason for this is that in a comparable collection, the secret key for each client is the same.

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 qualities of the renounced clients can be used by the client without the preset attributes in a similar gathering.Furthermore, we point out that by using Attribute Based Encryption plans to distributed storage

administrations, We can protect stored data as well as give fine-grained information access control. Unfortunately, when executing encryption and unscrambling operations, the Attribute Based Encryption scheme has a significant computation overhead. This distortion is particularly severe for lightweight electronics due to their compelled asset registration. To reduce the calculation cost for asset compelled devices, some cryptographic tasks with high computational burden were re-appropriated to cloud specialist organisations via intermediary re-encryption with a languid re-encryption procedure, structured a Key Policy- Attribute Based Encryption conspire with fine-grained information access control. The entry tree's root hub must be an AND door, and one of its children must be a leaf hub connected to the fake Attribute. The false credit must be included in the Attribute set of each datum report and will never be updated. Apart from the one related to the fictitious quality, cloud specialist organisation saves the whole private key segments for user's private key in their plan. Regardless, the plaintext for any information record is not learned by the cloud specialist business. When encrypting data before transferring it to an online cloud server, there are a few things to consider.

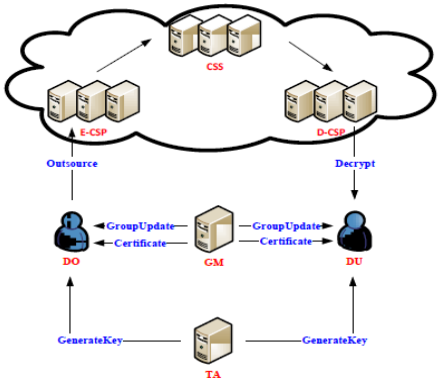
Proposed Algorithm:

Algorithm 2 PyramidFinder

Input: Set of items $\mathcal{I}$
Output: Dominance Pyramid $\mathcal{D}_{\mathcal{I}}$

$\mathcal{D}_{\mathcal{I}}[0] \leftarrow Sky(\mathcal{I})$
$\mathcal{Z} \leftarrow \mathcal{I} \setminus Skyline(\mathcal{I})$
$level \leftarrow 1$.
while $\mathcal{Z}$ is not empty **do**
  $\mathcal{D}_{\mathcal{I}}[level] \leftarrow Sky(\mathcal{Z})$
  for every item $j \in \mathcal{D}_{\mathcal{I}}[level]$ **do**
    for every item $i \in \mathcal{D}_{\mathcal{I}}[level-1]$ **do**
      if i dominates j **then**
        Add a link $i \rightarrow j$
        break
      end if
    end for
  end for
  $\mathcal{Z} \leftarrow \mathcal{Z} \setminus skyline(\mathcal{Z})$
  $level \leftarrow level + 1$
end while

Data that is safe Client denial is aided by Encryption of Cipher Text Using Policy Attributes; we anticipate a client's private key to be divided into two pieces. The first is about his permitted properties, and the second is about the gathering where he has a spot. Wwhen at least one data recipient departs from the collection, GM changes the assembling a key pair as well as existing clients' private keys. GM also applies for re-encryption duties from CSS in order to disclaim their access to the stored information [14]. The work procedure for all computations is depicted in the diagram below. The appropriate computations are included in aEncryption ofCipher Text Using Policy Attributes plot with client disavowal.



Performance Evaluation

Built on the Encryption of Cipher Text Using Policy Attributes technique, the Attribute Based Encryption Storage System. Lets the parameters |pars|, |msk|, |CT|, |L|, |T|, |SK|, |A| be the dimensions of the parameters open parameter, ace private key, figure message, the attribute, the attached data , the decoding key and the entrance structure, separately . The number of properties in a tunnel structure is denoted by l, and the amount of a credit set assigned to a customer's confirmations is denoted by k. Table 1 takes a gander at the limit multifaceted nature of our structure [15]. Clearly our structure is capable as far as the introduced accumulating overhead, which incorporates the essential encryption of Cipher Text Using Policy Attributes parts to the system open 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 amount 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 [20].

It isn't inconvenient to see that the computational essential for the customer in our structure is twice that in the covered up encryption of Cipher Text Using Policy Attributes 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 to the figure content recuperation if vital additionally, 2y mixing exercises are resolved to check paying little heed to whether the normaltext concealed in the redistributing sales has existed in the open cloud.

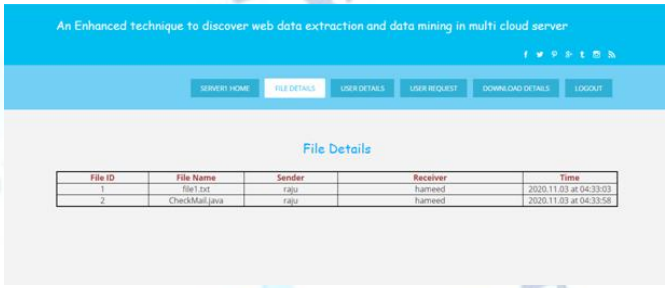
Variable attribute based Encryption

It shows cryptographic unrefined called versatile encryption of Cipher Text Using Policy Attributes, where a semi-accepted delegate is exhibited into the setting of encryption of Cipher Text Using Policy Attributes. 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 [22].

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 encryption of Cipher Text Using Policy Attributes outline works from a substitute viewpoint.

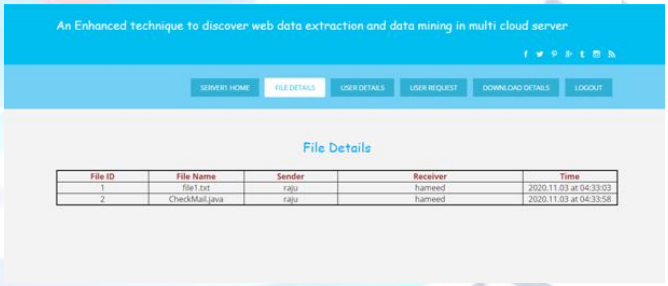
V. RESULTS

File Details from web server1



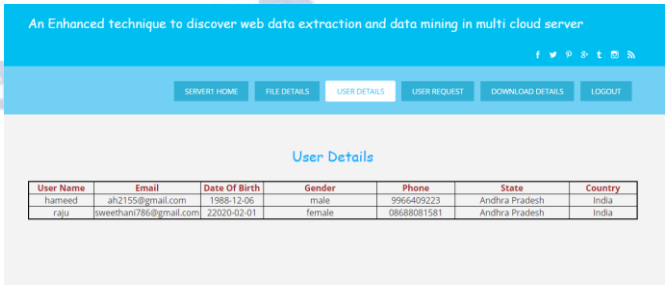
In the above screen server1 can check that the data is in correct format or not if its in virus format server won't allow to upload into the server.

File Details from web server2



In the above screen server2 can check that the data is in correct format or not if its in virus format server won't allow to upload into the server

User Detailed view from server



User file details after file search with encrypted keyword

In the above screen the server can check the user validity if it's not correct user then server won't allow to access privileges then he need to take permission from the server.

VI. CONCLUSION

We offer a new framework in this study called An Enhanced technique to Discover Web Data Extraction and Data Mining in Multi Cloud Server, which can support extracting data from various resources while avoiding guessing attacks, which are a common flaw in traditional public encryption and key search.In the future, our system might be expanded to provide insights on the essential skills and job distribution across industries and countries in the area, as well as a suggested tool for job seekers. Furthermore, in the lack of a reliable jobs list at the national level, similar approaches might be used to perform labour market research and take appropriate steps to prepare future employees to meet these needs.

REFERENCES

[1] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, "A new general framework for secure public key encryption with keyword search," in Proc. 20th Australasian Conf. Inf. Secur. Privacy (ACISP), 2015, pp. 59–76.

[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Secur. Privacy, May 2000, pp. 44–55.

[3] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2004, pp. 563–574.

[4] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. 13th ACM Conf. Comput. Commun.Secur.(CCS), 2006, pp. 79–88.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Int. Conf. EUROCRYPT, 2004, pp. 506–522.

[6] R. Gennaro and Y. Lindell, "A framework for password-based authenticated key exchange," in Proc. Int. Conf. EUROCRYPT, 2003, pp. 524–543.

[7] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in Proc. NDSS, 2004, pp. 1–11.

[8] M. Abdallaet al., "Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions," in Proc. 25thAnnu. Int. Conf. CRYPTO, 2005, pp. 205–222.

[9] D. Khader, "Public key encryption with keyword search based on K-resilient IBE," in Proc. Int. Conf. Comput. Sci. Appl. (ICCSA), 2006, pp. 298–308.

[10] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," IEEE Trans. Comput., vol. 62, no. 11, pp. 2266–2277, Nov. 2013.

[11] G. Di Crescenzo and V. Saraswat, "Public key encryption with searchable keywords based on Jacobi symbols," in Proc. 8th Int. Conf. INDOCRYPT, 2007, pp. 282–296.

[12] C. Cocks, "An identity based encryption scheme based on quadratic residues," in Cryptography and Coding. Cirencester, U.K.: Springer, 2001, pp. 360–363.

[13] J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in Proc. Int. Conf. Comput. Sci. Appl. (ICCSA), 2008, pp. 1249–1259.

[14] H. S. Rhee, J. H. Park, W. Susilo, and D. H. Lee, "Improved searchable public key encryption with designated tester," in Proc. 4th Int. Symp. ASIACCS, 2009, pp. 376–379.

[15] K. Emura, A. Miyaji, M. S. Rahman, and K. Omote, "Generic constructions of secure-channel free searchable encryption with adaptive security," Secur.Commun.Netw., vol. 8, no. 8, pp. 1547–1560, 2015.

[16] W. Byun, H. S. Rhee, H.-A. Park, and D. H. Lee, "Off-line keyword guessing attacks on recent keyword search schemes over encrypted data," in Proc. 3rd VLDB Workshop Secure Data Manage. (SDM), 2006, pp. 75–83.

[17] W.-C. Yau, S.-H.Heng, and B.-M. Goi, "Off-line keyword guessing attacks on recent public key encryption with keyword search schemes," in Proc. 5th Int. Conf. ATC, 2008, pp. 100–105.

[18] J. Baek, R. Safavi-Naini, and W. Susilo, "On the integration of public key data encryption and public key encryption with keyword search," in Proc. 9th Int. Conf. Inf. Secur. (ISC), 2006, pp. 217–232.

[19] H. S. Rhee, W. Susilo, and H.-J. Kim, "Secure searchable public key encryption scheme against keyword guessing attacks," IEICE Electron. Exp., vol. 6, no. 5, pp. 237–243, 2009.

[20] H. S. Rhee, J. H. Park, W. Susilo, and D. H. Lee, "Trapdoor security in a searchable public-key encryption scheme with a designated tester," J. Syst. Softw., vol. 83, no. 5, pp. 763–771, 2010.

[21] L. Fang, W. Susilo, C. Ge, and J. Wang, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," Inf. Sci., vol. 238, pp. 221–241, Jul. 2013.

[22] I. R. Jeong, J. O. Kwon, D. Hong, and D. H. Lee, "Constructing PEKS schemes secure against keyword guessing attacks is possible" Comput.Commun., vol. 32, no. 2, pp. 394–396, 2009.

[23] R. Cramer and V. Shoup, "Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption," in Proc. Int. Conf. EUROCRYPT, 2002, pp. 45–64.