PREVENTING DATA THEFT ATTACKS IN THE CLOUD USING FOG COMPUTING

PULICHINTHALA DIVYA TEJA[1], S. NAGA RAJU[2]
[1]Student, Master of Technology in Software Engineering, KITS, Warangal
[2]Associate Professor, KITS, Warangal

ABSTRACT: ***Cloud is basically a network based environment because it is a cluster of multiple servers within a network. Cloud computing enables multiple users for sharing common resources or computations, And cloud provides us variety of services, among them security is been considered has a prime factor. Cloud is based on pay- per-use model that is user will be paying for the resources he is going to use but not for the local resources such as storage and infrastructure due to this reason cloud has become the most existing technology in today's world. Many users will be out-sourcing their data in the cloud. By using cloud computing we will completely change the way of accessing the computers and storing their personal and business information. With this new cloud computing technology there would arise new data security challenges. The users who are having valid authority in the cloud are been treated has a insiders and all the remote users were been treated has a intruders, when an intruder stoles the accessing details of original user he get access into the cloud as a valid user. Now in this situation we are having two major challenges. First we need to distinguish real or fake user is been accessing the cloud and next we must protect the authorized users data from intruder.***

So for this purpose in this paper we propose a different approach of securing data in the cloud by using fog computing technology which is also been treated as a decoy technology or disinformation technology. So for this purpose we monitor data access patterns all the time and if any abnormal patterns were been detected we verify it by using security questions and if any abnormal data access patterns were detected we will provide a large amount of disinformation or bogus data by using decoy technology to the intruder by doing this we can protect the users data.

Index Terms :fog computing, intruders, access patterns, decoy technology, intruder detection system.

1. INTRODUCTION

Now a days many organizations are outsourcing their data in the cloud because security is been considered as a private issue. So that they can access their personal or business information from any place and many of the users are from internet. Even after taking some security measures we may undergo some security issues and we can identify these security issues easily if the intruder is malicious insider. Simply we trust the person and we store our confidential data in the cloud so this is considered has a top theft in cloud computing while most of the cloud users are well-aware of this threat.

While on the other side the attacks may also cause by the outsiders in this type of attacks they would stole the user's passwords and other accessing information and get access into the user's confidential data. In such state we can't identify weather he is authorized or unauthorized. So many measures were taken in preventing the data from unauthorized access and access control mechanisms but all encryption mechanisms were failed in preventing the data from attacks.

So in order to avoid this data threat attacks we are introducing a new concept called as **fog computing** technique in this approach here comes a combinations of two technologies search behavior and decoy technology we can identify the intruder by using intrusion detection system(IDS) which includes his search behavior and the security questions once after conforming him as intruder we will confuse the intruder with large amount of bogus or disinformation attack so now he can't identify the real and fake worth less data.

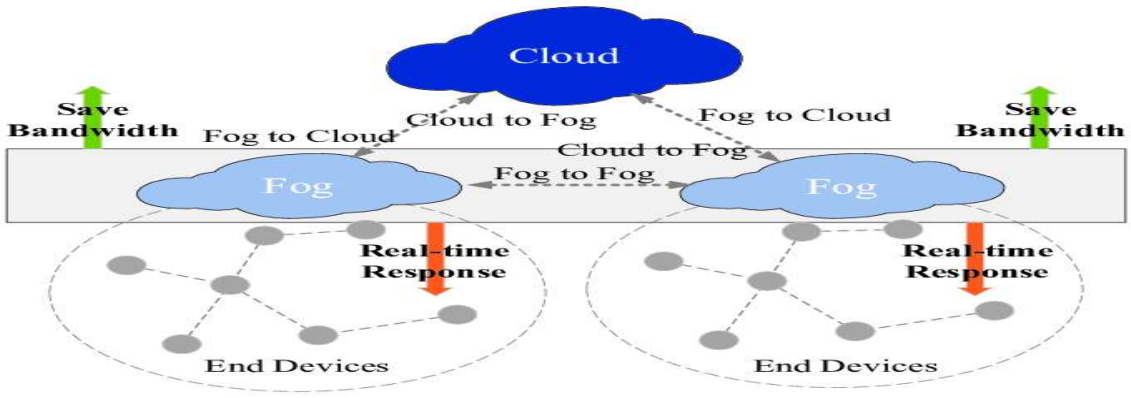

Figure 1: Fog Computing Architecture.

II. SECURING CLOUD WITH FOG

In today's world for all the enterprises such as small medium and large it has become a massive revolution for them to store and access their personal and business information. So with the existence of cloud computing technology they are outsourcing their personal and business information in the cloud as cloud provides us with wide variety of services such as security, speed, efficiency, reliability. Cloud stores a vast amount of data in it and provide to the user on demand and it is based on pay-per use model user can access his information any were through the internet.Fog computing is the term which was associated with "cisco" fog computing is also known as fogging, it is a distributed computing infrastructure in which some application services are been handled at the network edge in a smart devices and some of the applications.

Fog computing was mainly introduced to meet three primary goals:

1. To improve efficiency and trim the amount of data that required to be transmitted for processing storage and analysis.
2. Provide security and compliance to the data that is been transmitted over the cloud.

Fog networking consists of both data and the control plane were most of the networking take place in the data plane of the smart mobile or on the edge of the network in a gateway devices. The goal of fogging is to improve the efficiency and reduce the amount of data that need to be transported to the cloud for data processing, analysis and storage. This is often done for the efficiency reasons, but it may also carried out for security and compliance reasons. Fog computing is not a different form of technology, but it is just an extension of cloud computing technology.

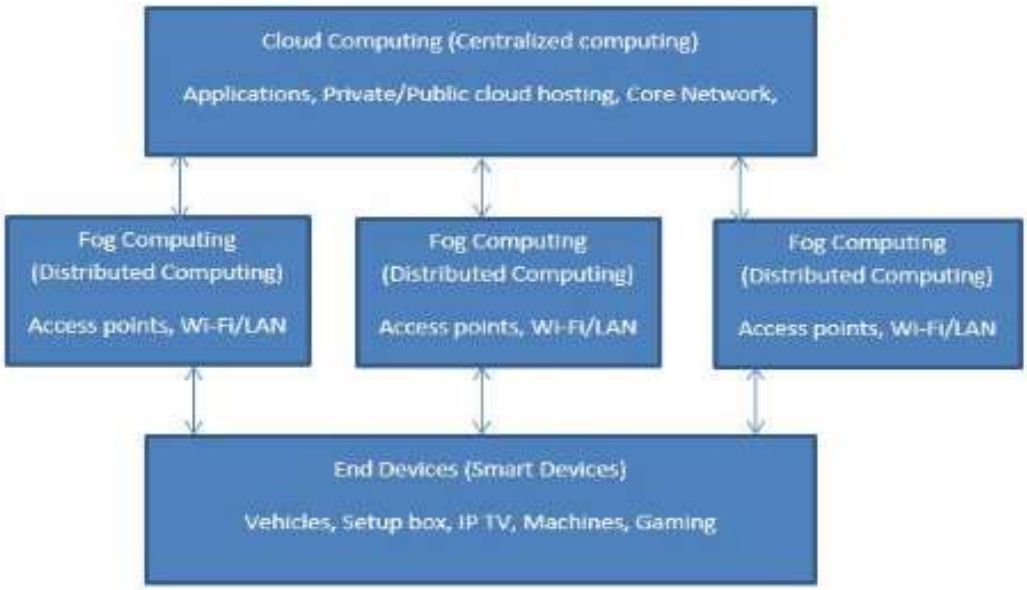

Figure 2: Securing Cloud Along With Fog.

As many enterprises were storing data in the cloud security has become the most serious problem known as data theft attacks, this attacks can be identified easily if the person is malicious insider simply we trust the cloud service provider and we outsource our data in the cloud and if any threat occurs to our data we can identify it by using intrusion detection system(IDS).

Although data in the cloud is encrypted, it stays for a length and it becomes vulnerable to the security threats here, fog provides the shortest possible distance between the client and server and reduces the risk of data security breach.

Many standard measures had been taken to protect data and secure. But all measures had been failed from time to time due to insider attacks, faulty implementation, buggy code. Developing trust worthy cloud computing environment is not enough. We need to reduce the attacks, so for this purpose we need to limit the stolen data we can achieve this through disinformation attacks.

We had proposed two security features:

1. User behavior profiling.
2. Decoy document.

USER BEHAVIOR PROFILLING:

User behavior is a technique which is used for identifying the behavior of the user all the time it keeps monitoring the behavior of the user continuously and keep track of the user's behavior system. And check for any abnormal data access patterns. In a User profiling technique we will be monitoring how when and how often a files or data were been accessed by the user in the cloud. Such type of normal user's behavior can be continuously checked to detect any of the abnormal data access patterns. To be explained clearly when any of the cloud user get access into the cloud then our system will keep detecting the behavior of the user on the following basis:

1. Login time
2. Duration of accessing the file
3. File upload time

4. File download time
5. No of files downloaded
6. No of files uploaded
7. Logout time.

This method of behavior based security is commonly seen in fraud detection applications such profiles would normally include volumetric information and accessing details about files.

System will be comparing all above mentioned basis with the pre- defined data sets which is already stored in the database depending on the user's behavior and identifies user is authorized or not according to the search behavior data will be sent to the user.

DECOY TECHNOLOGY:

In this decoy technology we will be producing a different approach of securing data in the cloud by using offensive decoy technology. A decoy is a document of set of files, directories, documents which appear similar to that of the original documents however the aim of the decoy is to provide the decoy document by hiding the real data without hacking by an intruder. So we can define it as fake system which appears to be as a real system.

A decoy system can be grouped into several steps:

1. Prevention
2. Detection
3. Response

Prevention is the first thing that we must be considered in the system model we should not allow the hacker to hack the system for this purpose there are many security measures one among them is firewall. It can be used to control network traffic and put some rules to block it. And by using security questions, by putting strong passwords are some of the common well known techniques for security prevention. And one important thing is that encrypting the data and making it unable to read so by this way we can protect the data.

Detection is the technique which is used for detecting any malicious intruder is trying to access the data. We can detect the DATA THEFT ATTACKS in the cloud by intrusion detection system (IDS). This is only used to detect the system is hacked but we cannot stop the intruder from hacking. At this point decoy documents or honey pots are more valuable for tracking the activity.

Response: At this stage we are sure that our system is been hacked and we should respond to the system. This is the place where we launch a disinformation or bait information attack by providing the large amount of disinformation to intruder by securing the users real data.

We use this technology of disinformation attack against malicious insider preventing them from distinguishing fake data from real worthless data..

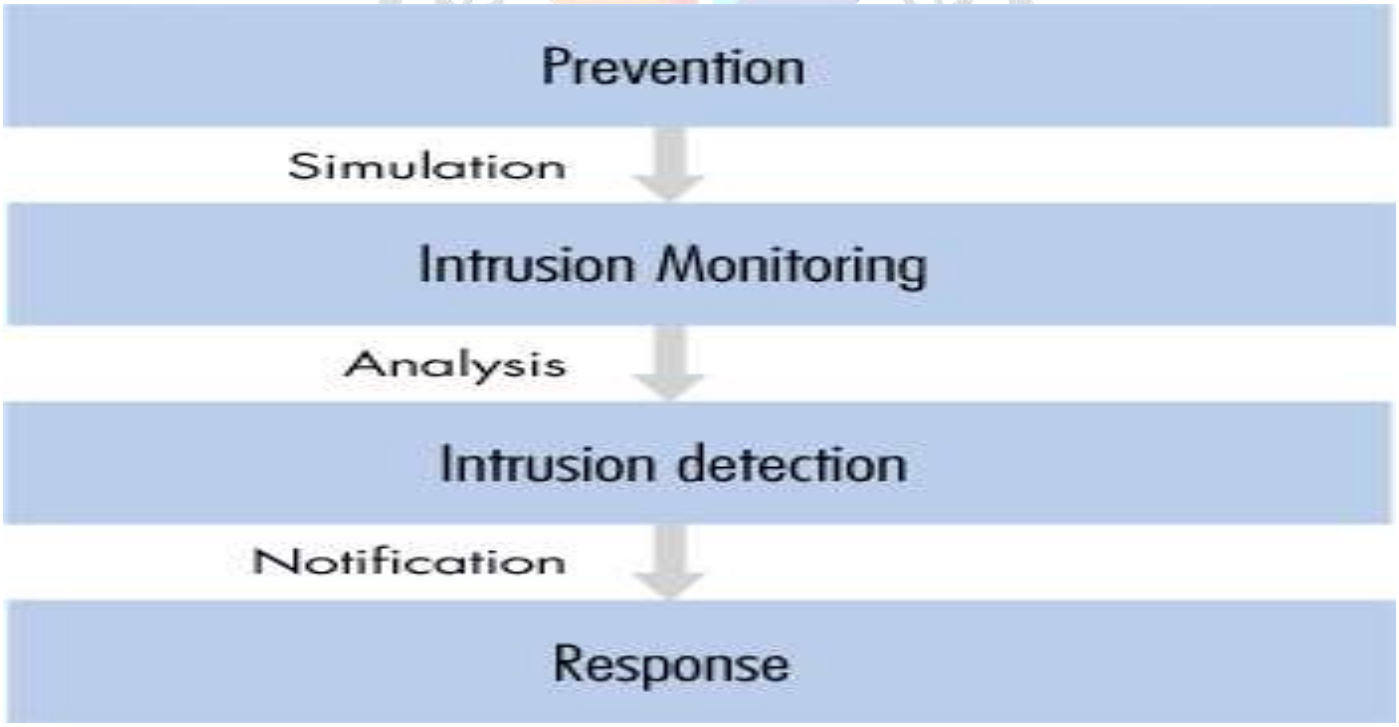

Figure 3: Information Security Phases.

III. COMBING USER BEHAVIOUR AND DECOY TECHNOLOGY

By providing the combination of these two security features we will be providing unpredictable level of security in the cloud. There is no such measure which provides this level of security features. We had been applied this concept to detect illegitimate data access to the data which is stored in the local file system by masquerader. The attacker tries to impersonate legitimate users after stealing their credentials. Our experimental results in a local file system shows that by combining both techniques we can yield better results in the cloud environment.

USER BEHAVIOR PROFILING:

In user behavior profiling we will continuously monitoring the user's behavior and we track all this information and stores in the database.
An authorized user search behavior would be completely different when compared to that of the unauthorized user or an intruder. A legitimate user he knows exactly the location of the specific file that had been stored in system so his search behavior would be simple. And when intruder tries to access the file then his search behavior would be totally different when compared to normal user.

DECOY TECHNOLOGY:

In this decoy technology their will be decoy files also known as honey files or honey pots which will be same as that of original data. The intruder he can't make difference of original and fake worthless data.
By using intrusion detection system we are detecting the intruders, this analysis include search behavior and security questions so once after knowing that intruder had been accessed the file system. In this file system we will placing some traps and this traps include some documents, files, which were been placed in egregious places the intruder who is not aware of this files or document click on these false document believing that they had been ex-filtered the use full information. When a false document is been downloaded an alert message will be generated. With this activity the system notify of an illegal activity by this way we can protect our authorized user's data.

$Pa=M(P, P')=\Delta E \leq T$

Where T can be determined as performance parameter or threshold value.

$Pi=M(P, P')$

$Pi=1-Pa$

Intruder is aware of knowing the exist

$Vi = Action(Vi \square 1)$ where $Vj \neq Vi, j < i$

An action may be command or function that displays files and documents

$Pa[Access\ u,m= 1] \geq €$

Normal legitimate user accessing the file

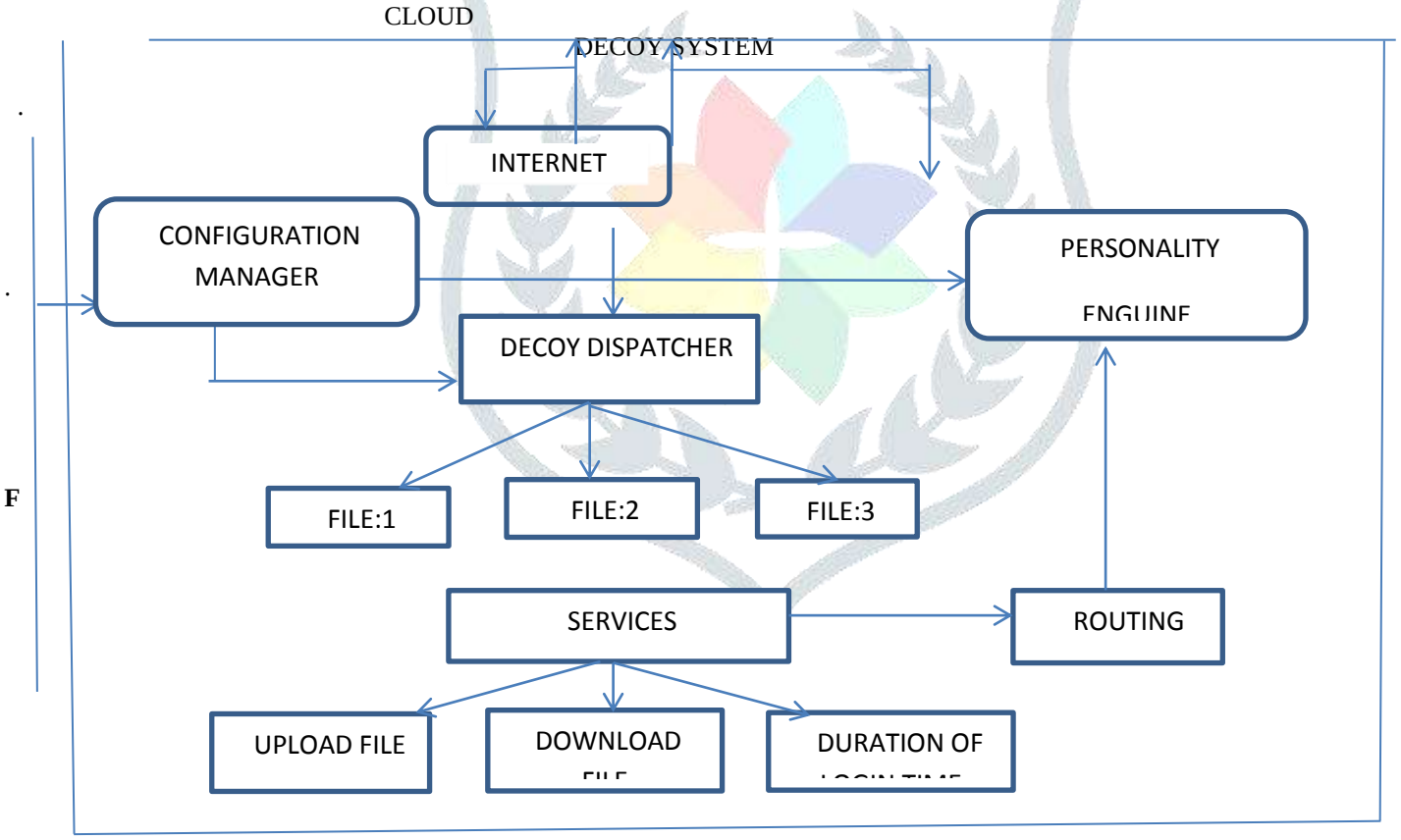

Figure 4: DECOY STRUCTURE.

ADVANTAGES OF PLACING DECOYS IN THE FILE SYSTEM:

1. Validating the authorized data when abnormal data access patterns were noticed.
2. Confusing the attackers with disinformation attacks.
3. Sending bogus files when an intruder is detected.

BLACKHAT MOTIVIES

BLACKHAT motives is a technique which is used to keep track about the information of unauthorized access to an authorized user's data and add the count according to the blacklist count. Only the user who is authorized only have an authority to clear the blacklist count but not to the unauthorized user.

When an unauthorized user tries to clear the list the system would send an OTP to the authorized user.

$Pi[d \rightarrow M : ALERTA,D=1] \geq €$

An alert is generated when decoy files are been exploited.

ALERTA,D=1 Denotes that an alert is generated when decoy document is generated.

d is detected with probability € when it is equal to 1.

NUMBER OF PLACED DECOYS	NUMBER OF USERS	NUMBEROF DECOY ACCESS
15	10	5
20	15	10
35	20	15
40	30	20

DT TABLE 1: NUMBER OF DECOYS AND DECOY ACCESS.

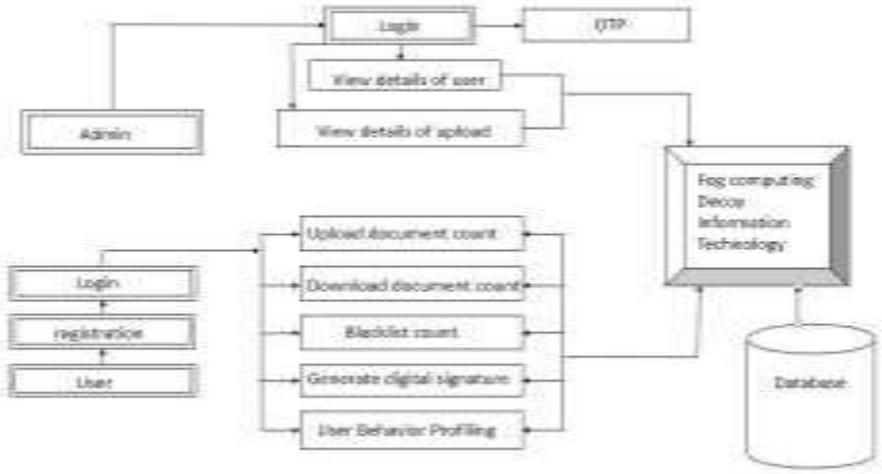

FIGURE 5: Data Flow Diagram.

MATHAMATICAL MODEL

Let G be the superset of all sets.

G ≡ {input, output, file operations, intruder detection, decoy files}

Where,

Input is set of parameters provided as input to the system.

Input ≡ {U, S, DS, F}

U is set of users. It is infinite set of users.

U ≡ {U1, U2, U3……Un}

S is set of servers. It is finite set of servers.

S ≡ {S1}

DS is set of dataset parameters.

DS ≡ {P1, P2, P3, P4, P5}

P1 ≡ Session Time

P2 ≡ Duration

P3 ≡ File upload count

P4 ≡ File Download count

P5≡ Blacklist count

F is set of files. It is Infinite set of files.

F ≡ {F1, F2, F3……,Fn}

Output is set of results.

Output ≡ { Legal user/Unreal user, Decoy document, Alert user via mail, OTP via SMS}

File Operations is set of functions.

Operations ≡ {Op1, Op2, Op3, Op4, Op5, Op6, Op7,Op8, Op9}

Op1 ≡ users request will be processed
Op2 ≡ Load user profile
Op3 ≡ comparing with the recorded search behavior patterns
Op4 ≡ if pattern match
Op5 ≡ Fetch file
Op6 ≡ if pattern does not match treat the user as an intruder.
Op7=provide decoy document/bait information
Op8 ≡alert users
Op9 ≡ Update log, Blacklist

INTRUDER DETCTION

IDS= {comparing with search behavior and security questions}
Decoy Files {DF}
DF= {providing intruder with large amount of bogus information}

IV. CONCLUSION

In this paper we define a fog computing which is totally a unique technology to protect the cloud by securing the user's personal and the business data. So for this purpose we keep track of user access patterns and also search behavior by continuously monitoring the user's data. In this we provide access to user's data by login details and also by using security questions which would be only known to the cloud users. If access is found authorized we provide original document of the user. If in case the access is been found unauthorized, the users actual data will be saved by provide the duplicate data by using decoy technology. This technology will add a level of securing data in the cloud

REFERENCES

[1] Ben-Salem M, and Stolof D. Keromytis, "fog computing: Mitigating insider data theft attacks in the cloud" IEEE symposium on security and privacy workshop.
[2] cloud Security Alliance,"top threat to cloud computing V1.0," March 2010.[online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
[3] D. Takahashi. "French hacker who leaked Twitter documents to techcrunch is based," march 2010.[online] Available:http://venturebeat.com/2010/03/24/French-hackers-wholeaked twitter-documents-to-tech-crunch is based.
[4] D.Danchev, "zdnet: French hacker gain acessto twitter's admin panel," april 2009.[online].available: http://www.zdnet.com/blog/security/french-hacker- gains-access-totwitters-admin-pannel/3292.
[5] P.Allen, "Obama's twitter password revealed after French hacker arrested for breaking into u.s president's account," march 2010.[online] available http://www.dailymail.co.uk/news/article-1260488/Barack- Obamas-Twitter-password-revealed-French-hacker-arrested.html.
[6] Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud Position Paper Salvatore J. Stolfo Computer Science Department Columbia University New York , NY, USA Email: sal@cs.columbia.edu Malek Ben Salem Cyber Security Laboratory Accenture Technology Labs Reston, VA, USA Email: malek.ben.salem@accenture.com Angelos D. Keromytis Allure Security Technologies New York , NY, USA
[7] B. Srinivas, Gadde Ramesh, Shoban Babu Sriramoju, "An Overview of Classification Rule and Association Rule Mining" in "International Journal of Scientific Research in Computer Science, Engineering and Information Technology", Volume-3, Issue-1, February-2018, 643-650, [ISSN : 2456-3307]
[8] B. Srinivas, Shoban Babu Sriramoju, "Managing Big Data Wiki Pages by Efficient Algorithms Implementing In Python" in "International Journal for Research in Applied Science & Engineering Technology (IJRASET)", Volume-6, Issue-II, February-2018, 2493-2500, [ISSN : 2321-9653]
[9] Shoban Babu Sriramoju, "Analysis and Comparison of Anonymous Techniques for Privacy Preserving in Big Data" in "International Journal of Advanced Research in Computer and Communication Engineering", Vol 6, Issue 12, December 2017, DOI 10.17148/IJARCCE.2017.61212 [ISSN(online) : 2278-1021, ISSN(print) : 2319-5940]
[10] Ajay Babu Sriramoju, Dr. S. Shoban Babu, "Analysis on Image Compression Using Bit-Plane Separation Method" in "International Journal of Information Technology and Management", Vol VII, Issue X, November 2014 [ISSN : 2249-4510]
[11] Shoban Babu Sriramoju, "Mining Big Sources Using Efficient Data Mining Algorithms" in "International Journal of Innovative Research in Computer and Communication Engineering" Vol 2, Issue 1,January 2014 [ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]
[12] Ajay Babu Sriramoju, Dr. S. Shoban Babu, "Study of Multiplexing Space and Focal Surfaces and Automultiscopic Displays for Image Processing" in "International Journal of Information Technology and Management" Vol V, Issue I, August 2013 [ISSN : 2249-4510]
[13] Monelli Ayyavaraiah, "Review of Machine Learning based Sentiment Analysis on Social Web Data" in "International Journal of Innovative Research in Computer and Communication Engineering" Vol 4,Issue 6,March 2016 [ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]
[14] Monelli Ayyavaraiah, " A Study on Large-Scale Cross-Media Retrieval of Wikipedia Images towards Visual Query and Textual Expansion" in "International Journal for Research in Applied Science and Engineering Technology", Volume-6, Issue-II, February 2018, 1238-1243 [ISSN : 2321-9653], www.ijraset.com

[15] Monelli Ayyavaraiah, "Nomenclature of Opinion Miningand Related Benchmarking Tools" in "International Journal of Scientific & Engineering Research" Vol 7,Issue 8, February 2018, [ISSN 2229-5518]
[16] Siripuri Kiran, 'Decision Tree Analysis Tool with the Design Approach of Probability Density Function towards Uncertain Data Classification', International Journal of Scientific Research in Science and Technology(IJSRST), Print ISSN : 2395-6011, Online ISSN : 2395-602X,Volume 4 Issue 2, pp.829-831, January-February 2018. URL : http://ijsrst.com/IJSRST1841198
[17] Ajmera Rajesh, Siripuri Kiran, " Anomaly Detection Using Data Mining Techniques in Social Networking" in "International Journal for Research in Applied Science and Engineering Technology", Volume-6, Issue-II, February 2018, 1268-1272 [ISSN : 2321-9653], www.ijraset.com