# Cloud Computing Based Forensic Analysis for Network Security System

**Balkrushna B. Jagadale**[1], **Dr. Sujatha Terdal**[2]

[1]Department of Computer Science & Engineering M.Tech.(CSE),
Poojya Doddappa Appa College of Engineering, Gulbarga, Karnataka, India

[2]Associate Professor, Department of Computer Science & Engineering,
Poojya Doddappa Appa College of Engineering, Gulbarga, Karnataka, India

**Abstract**: ***Internet and network security has been one of the most integral parts of private and public network. In this work we have proposed a real time cloud based security extension that authenticates the user through his Gmail credentials and scans his recent mail through reading RSS feed of the mail service offered by Google. User can choose to blacklist particular keywords or domains. Keywords and domains blacklisted by multiple users are globally defined as threat and every user's mails are filtered based on both local as well as global definition. Further our system scans the network packets through WiFi virtual adapter using Winpcap network monitoring system and makes the statistical data available globally by integrating the logging service with Thingspeak logging and visualizing services.***

**Keywords:** Cloud computing, Anti-phishing, Email Security and Network Security System.

## 1. Introduction

Network security is integral part of computer networks. Different types of security services are being developed both at commercial level as well as a research method for protecting user's interest, identity and data over a computer network. However the distributed nature of network access and evolution of Cloud environment has enabled the user to access his data, emails and network services with a variety of devices. This makes the security extensions particularly difficult as every system the user access needs to be updated to the current point with metadata like virus definitions, intrusion patterns and so on. Current state of art does not offer network security as service. The stand alone nature of the network security principles make is extremely difficult to efficiently access the service over wide range of network and devices. Hence there is a dire need for security techniques to be extended over the cloud that can be seamlessly adopted over wide verity of network and devices. In this work we propose to solve this critical network security problem by offering cloud based network security for email security and network security through network monitoring. Email security links real time Gmail service with custom cloud based knowledge base which is personalized. In-server mining links multiple user's knowledgebase to offer a global blacklist definition. Network monitoring services logs current network activity and offers packet statistics as a global online graph through Thingspeak which can be visualized from variety of devices. Any sudden traffic burst like youtube and torrent access can be tracked as an event over the graph which hints the network administrator to take appropriate action against the device or IP address found violating the network norms.

## 2. Related Work

Security is one of the big issue in cloud computing. Till today there has a lot of work on security but it's not up to that status. Email security also has an issue with the phishing attack, malicious activities, etc. We survey previous and related work in remote forensic acquisition, forensic data collected by providers, and methods for storing content on untrusted platforms.

“Categories of digital investigation analysis techniques based on the computer history model”, Brian D. Carrier, Eugene H. Spafford [1], have used the model based on the history of a computer to define categories and classes of analysis techniques.

“A second generation computer forensic analysis system”, Daniel Ayers [2], has discuses the limitations of first generation computer forensic tools. Several metrics for measuring the efficacy and performance of computer forensic tools are introduced.

“Identifying Vulnerable Websites by Analysis of Common Strings in Phishing URLs”, Brad Wardman, Gaurang Shukla, and Gary Warner[3], has created and suggest a method for identifying common attack methods, as well as, help inform webmasters and their hosting companies in ways that help them to defend their servers. Method involves applying a Longest Common Substring algorithm to known phishing URLs, and investigating the results of that string to identify common vulnerabilities, exploits, and attack tools which may be prevalent among those who hack servers for phishing.

“Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform” Josiah Dykstra, Alan T. Sherman[4], have described the design, implementation, and evaluation of FROST three new forensic tools for the OpenStack cloud platform. Implementation for the OpenStack cloud platform supports an Infrastructure-as-a-Service (IaaS) cloud and provides trust worthy forensic acquisition of virtual disks, API logs, and guest firewall logs.

"Enhancement of Existing Tools and Techniques for Computer Forensic Investigation", Gouthami Velakant, Aditya Katuri[5], has done work on data retrieval the most important part of computer Forensic investigation. The main area from which data can be retrieved is file slack. In this we discuss different tools and techniques of searching and retrieving the data and enhancements to the existing tools for better performance.

"Securing Digital Forensics on Cloud Computing through Log based Accession", Raju Kadari, Janapati Venkata Krishna[6], has propose a perspective which using logs model to build a forensic friendly system. Using this forensic-friendly system model we can quickly gather information from cloud computing for some kinds of forensic purpose and this perspective decrease the complexity of those kinds of forensics.

"Forensic Investigation in Cloud Computing Environment", Agreeka Saxena, Gulshan Shrivastava, Kavita Sharma[7], has been in its boom stage since a long time. Although the exact definition of Cloud Computing have a cloudy appearance in the Information Technology environment -in this paper, the related definition of cloud computing along with computer forensic has been explain. Various computer forensic measures and merits are explained.

"The Digital Forensic Research: Current State-of-the-Art", Sriram Raghavan has[8], has witnessed significant technological advancements to aid during a digital investigation. Many methodologies, tools and techniques have found their way into the field designed on forensic principles.

"Computer Forensics using Bayesian Network: A Case Study", Michael Y.K. Kwan, K.P. Chow, Frank Y.W. Law, Pierre K.Y. Lai[9], like the traditional forensics, computer forensics involves formulation of hypotheses grounding on the available evidence or facts. Though digital evidence has been statutory witnesses for a span of time, it is a controversial issue that conclusions drawn from revealed digital evidence are subjective views without scientific justifications.

## 3. Problem Statement

Phishing was a term originally used to describe email attacks that were designed to steal your online banking username and password. However, the term has evolved and now refers to almost any email-based attack. Phishing uses social engineering, a technique where cyber attackers attempt to fool you into taking an action. These attacks often begin with a cyber criminal sending you an email pretending to be from someone or something you know or trust, such as a friend, your bank or your favorite online store. These emails then entice you into taking an action, such as clicking on a link, opening an attachment or responding to a message. Cyber criminals craft these emails to look convincing, sending them out to literally millions of people around the world. The criminals do not have a specific target in mind, nor do they know exactly who will fall victim. They simply know the more emails they send out, the more people they may be able to fool. The objective of this work is to provide real time Email Security and Network monitoring service using suitable cloud integration such that the service of an user can be used from different machines without the need to import the settings from one system to another.

Every email providers come with spam filters and virus scanners that release the mails after through scanning. However advertisement mails and certain business and promotion mails still makes it through user inbox. These junk mails are not filtered by the service providers. In order to personalize the mail delivery, the user needs preference definition that spans across different devices and emails.

## 4. Proposed Work

### 4.1 Proposed System

In this work we have proposed a real time cloud based security extension to meet the challenge of changing network fundamentals and data access. The proposed work provides two distinct services: Email Security and Network security as cloud based service. The work integrated Email service of Gamil and authenticates user using his Gmail credential. Once authenticated, the system scans new mail's metadata as a background process by reading the RSS feed of the user's Gmail account. It then links a cloud based keyword service with the scanner which enables the user to filter his mails based on predefined keywords he has chosen. User can blacklist particular mail IDs and keywords depending upon his preference. Any mail ID and keyword if blacklisted by multiple users, become automatically global filter for all the users.

The system also scans network packets with the help of Winpcap service by monitoring the virtual adapter through which the system is connected with internet. Packets and their information like source address, destination address, port, TTL, packet length is logged. A statistical process calculates the statistics based on packet length and bandwith and logs the data to real cloud visualization service offered by Thingspeak. Network administrator can view the pattern remotely from his mobile or handheld devices. This process also shows the event triggers when sudden burst of traffic is released in the network.

### 4.2 Architecture

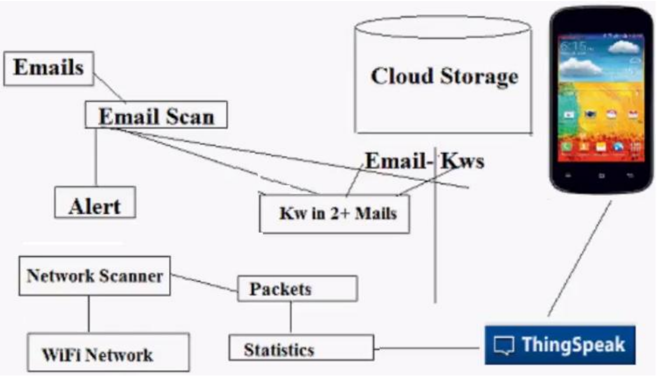


**Figure 1:** Architecture of proposed system.

Proposed work contains following major modules. In this subsection we present a brief overview of the modules which are:

a) **Email Scanner:** This module authenticates the application by using user's Google credentials. Once the account is authenticated, current emails are being read as RSS feed. RSS being an open XML format, needs parsing for data extraction. Using LinQ based XML parser, fields of mails are parsed and displayed in GUI.

b) **Preference Definition:** User can define his list of preferred keywords and also blacklist unwanted mail IDs. These preferences are stored through open cloud service provided by Grasshoppernetwork.com. The preferences are aggregated at the server and the list of keywords being blacklisted by more than one user becomes global preference and is available with all the users.

c) **Alert Manager:** Alert manager checks links the preference definition in the mails and marks the emails with red annotation.

d) **Network Scanner:** Network scanner is based on Winpcap packet capturing service. The scanner can tap into a specific access port and read all the packets being exchanged through the port. We configure the scanner with Microsoft's virtual miniport which is an adapter through which WiFi network is accessed. Thus the system is capable of watching all the packets being exchanged over the WiFi network.

e) **Statistics Manager:** Statistics manager extracts packet length and total length statistics of the packets as well as time bound standard deviation of the packets.

f) **Cloud Logger:** Cloud logger connects to Thingspeak API services through API key generated for a Thingspeak channel. Periodic packet statistic obtained from statistic manager is logged to thingspeak channel. This data is remotely viewed just by logging to the channel URL.

### 4.3 0th Level System Data Flow Diagram

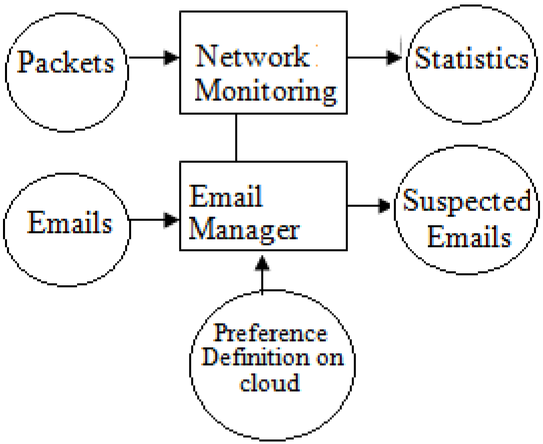


**Figure 2:** 0th Level System Data Flow Diagram

In above figure network monitoring is done with the Winpcap packet capturing. It will scan packets from incoming network and will show the statistic. Email manager will maintain the user authentication and pulls the inbox of that authenticated email id. Preference definition on cloud is related with phishing words stored over cloud for that email id. Using that keywords suspected mails are searched.

### 4.4 1st Level System Data Flow Diagram

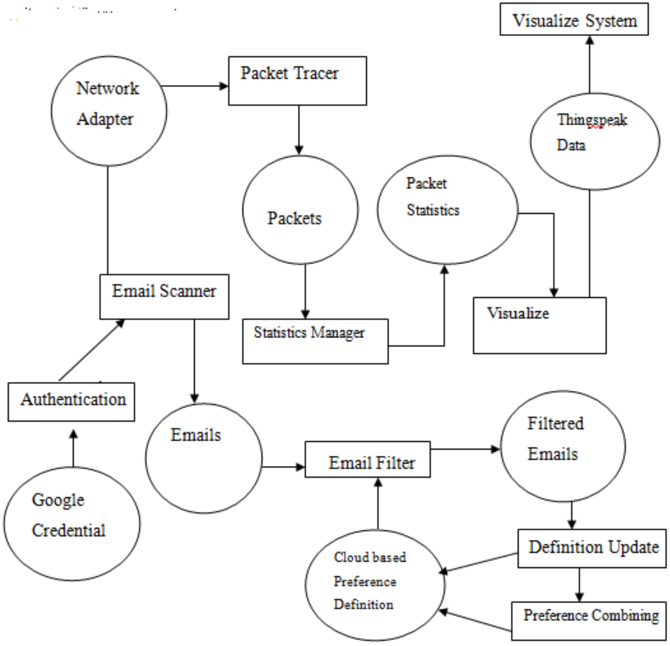


**Figure 3:** 1st Level System Data Flow Diagram

This data flow diagram shows the overall execution of proposed system. Using the Google credential authentication for email account is performed. Email scanner will scan the inbox and pull inbox mails to the filter. After that user can define his list of preferred keywords and also blacklist unwanted mail IDs. These preferences are stored through open cloud service provided by Grasshoppernetwork.com. Using this suspected that is filtered emails are found out. It's also possible to add new phishing keyword to cloud preference definition using definition update. And it will visualize to us using dynamic graph. By choosing an appropriate network adapter packet tracing of wifi network is starts. Statistics manager extracts packet length and total length statistics of the packets as well as time bound standard deviation of the packets. Thingspeak API services through API key generated for a Thingspeak channel. This is using the channel number 40629. Periodic packet statistic obtained from statistic manager is logged to thingspeak channel. This data is remotely viewed just by logging to the channel URL.

### 4.5 System Data Flowchart Diagram

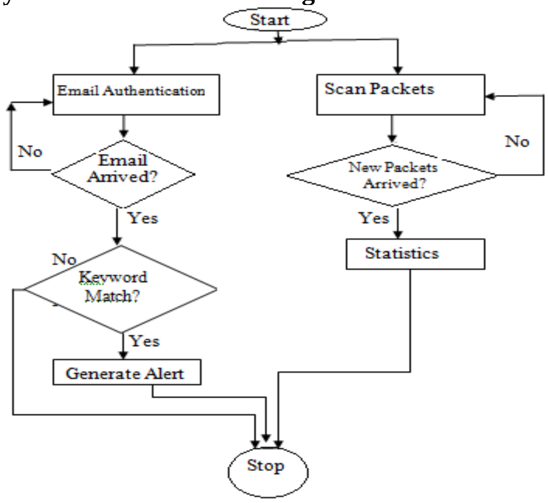
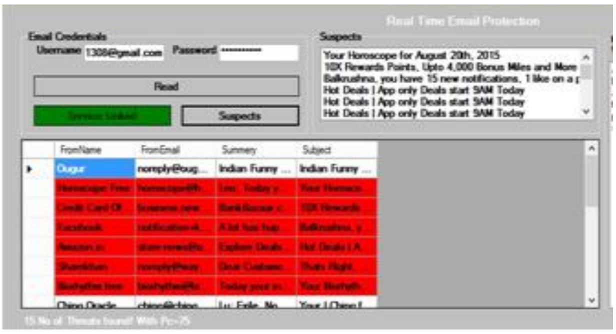


**Figure 4:** System Data Flowchart diagram

In first part execution starts with email authentication. Then it will check for the received mails if it is not means scan for emails again. After pulling the mails keyword matching is performed to find out the suspected phishing mails among that pulled mails. It will use the keywords that are stored over cloud based security system. Then it will end the execution for first part with suspected mails count or no suspected mails if not find means. In second part of execution by choosing an appropriate adapter it will scan for the packet arriving. For every new packet arriving it will show the statistic and again scan for the new packets.

## 5. Results

It gives the suspected phishing mails in our email inbox highlighted with red color. It uses the phishing keywords that are stored in center based cloud security system.



Your Horoscope for August 20th, 2015
10X Rewards Points, Upto 4,000 Bonus Miles and More
Balkrushna, you have 15 new notifications, 1 like on a p
Hot Deals | App only Deals start 9AM Today
Hot Deals | App only Deals start 9AM Today
Hot Deals | App only Deals start 9AM Today

| | FromName | FromEmail | Summery | Subject |
|---|---|---|---|---|
| ▶ | Ougur | noreply@oug... | Indian Funny ... | Indian Funny ... |
| | Horoscope Free | horoscope@h... | Leo : Today y... | Your Horosco... |
| | Credit Card Of | bizserene.new | BankBazaar c... | 10X Rewards |
| | Facebook | notification+k... | A lot has hap... | Balkrushna, y |
| | Amazon.in | store-news@... | Explore Deals... | Hot Deals I A |
| | [illegible] | noreply@way | Dear Custome... | Thats Right |
| | Biorhythm free | biorhythm@... | Today your m... | Your Biorhyth |
| | China Oracle | chino@chino... | Lu: Exile. No | Your I Ching f |

15 No of Threats found! With Pc-75

**Figure 5:** Phishing Mail Detected

This also allow to add suspected email id and domains into blacklist. By selecting the suspected mail the window named sender blacklist it will show the id and name of sender and by clicking on blacklist that id will be add to the blacklist and again you won't get phishing mail from same id.

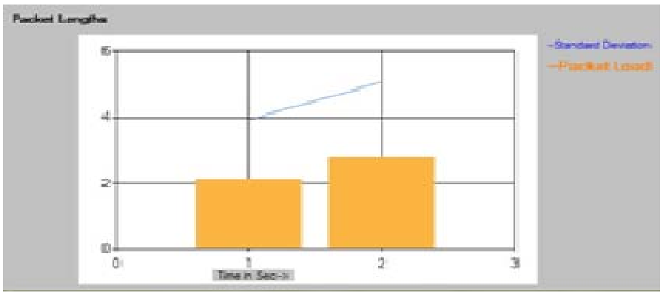


**Figure 6:** Smooth Network Analysis

It shows that the analysis of network when the traffic is smooth that no load time for network. It gives a stable and equal statistics for wi-fi network. It uses the standard deviation of network and also the packet load against the time in second.

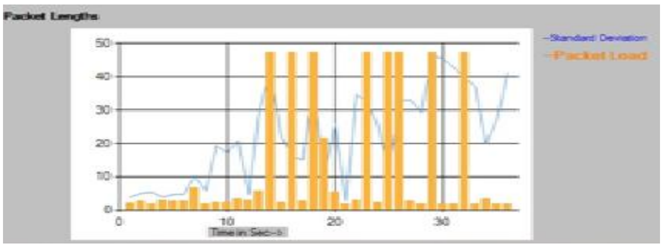
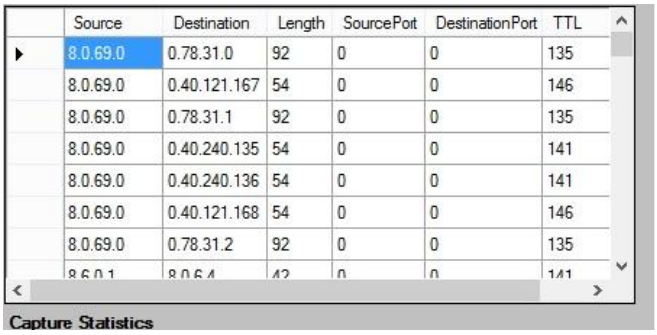


**Figure 7:** Brusty Traffic Analysis

As the traffic over network get increased the graph also changes and give analysis with respect to that particular time network load. Statistical Manager extracts packet length and total length statistics of the packets as well as time bound standard deviation of the packets. It also gives the Source and Destination IP address ,Packet Length, Source and destination Port and Time-To-Live(TTL) .



| | Source | Destination | Length | SourcePort | DestinationPort | TTL |
|---|---|---|---|---|---|---|
| ▶ | 8.0.69.0 | 0.78.31.0 | 92 | 0 | 0 | 135 |
| | 8.0.69.0 | 0.40.121.167 | 54 | 0 | 0 | 146 |
| | 8.0.69.0 | 0.78.31.1 | 92 | 0 | 0 | 135 |
| | 8.0.69.0 | 0.40.240.135 | 54 | 0 | 0 | 141 |
| | 8.0.69.0 | 0.40.240.136 | 54 | 0 | 0 | 141 |
| | 8.0.69.0 | 0.40.121.168 | 54 | 0 | 0 | 146 |
| | 8.0.69.0 | 0.78.31.2 | 92 | 0 | 0 | 135 |
| | 8.6.0.1 | 8.0.6.4 | 42 | 0 | 0 | 141 |

Capture Statistics

**Figure 8:** Captured Statistic

Thingspeak API services through API key generated for a Thingspeak channel. Periodic packet statistic obtained from statistic manager is logged to thingspeak channel. This data is remotely viewed just by logging to the channel URL.

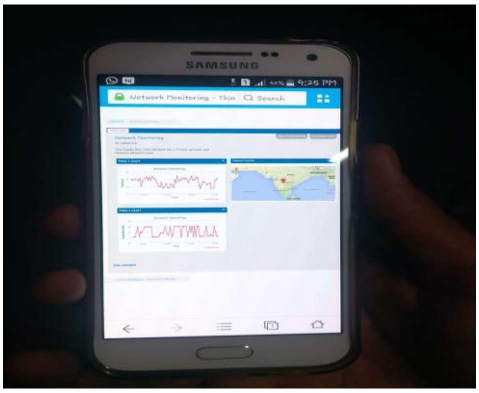


**Figure 9:** Mobile View Over Thingspeak

## 6. Conclusion

Network monitoring, network security and email security is not new as far as research and architecture is concerned. However new development in computation and changing distributed nature of network access leads to new challenges in this area. User's security preferences and settings are needed to be available globally such that they can be accessed from different platforms. Even though new techniques are developed for more efficient network security extensions, cloud based techniques are needed to meet the challenges. The same goes true even for network monitoring system.

In this work we have proposed a unique cloud based system that integrates email security with network monitoring and event trigger based security system. The work is integrated with cloud based services for user preference integration for email filtering. The system also offers real time packet statistics logging through Thingspeak such that the access statistics is available over different devices. Results show that the technique detects the phishing attack and prevents the malicious activities.

## 7. Future Scope

The system can be improved by incorporating other techniques like malicious node and content detection methods and data security techniques with the proposed architecture. Such an improvement would transform the proposed technique to more complete network security extension.

## References

[1] Brian D. Carrier, Eugene H. Spafford, Categories of digital investigation analysis techniques based on the computer history model digital investigation 3 S (2006) S121 – S130, Published by Elsevier Ltd.
[2] Daniel Ayers, A second generation computer forensic analysis system, digital investigation 6 (2009) S34 – S42.
[3] Brad Wardman, Gaurang Shukla, and Gary Warner, Identifying Vulnerable Websites by Analysis of Common Strings in Phishing URLs, received June 25th ,2009, by the Edwards Byrne Memorial Justice Assistance Grant Program.
[4] Josiah Dykstra, Alan T. Sherman, Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform, Digital Investigation 10 (2013) S87–S95.
[5] Gouthami Velakant, Aditya Katuri, Enhancement of Existing Tools and Techniques for Computer Forensic Investigation, International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 161-164.
[6] Raju Kadari, Janapati Venkata Krishna, Securing Digital Forensics on Cloud Computing through Log based Accession, International Journal of Computer Trends and Technology (IJCTT) – volume 16 number 2 – Oct 2014.
[7] Agreeka Saxena, Gulshan Shrivastava, Kavita Sharma, Forensic Investigation in Cloud Computing Environment, The International Journal of FORENSIC COMPUTER SCIENCE, IJoFCS (2012) 2, 64-74.
[8] Sriram Raghavan, Digital Forensic Research: Current State-of-the-Art, Queensland University of Technology Brisbane, Queensland 4000, AUSTRALIA s.raghavan@qut.edu.au.
[9] Michael Y.K. Kwan, K.P. Chow, Frank Y.W. Law, Pierre K.Y. Lai, Computer Forensics using Bayesian Network: A Case Study, HKU CS TECH REPORT TR-2007-12.
[10] W.H.Allen,Computer Forensics,IEEE Security & Privacy,Volume: 3, Issue: 4, Page(s): 59 –62, 2005.
[11] F.Raynal, Y.Berthier, P.Biondi, D.Kaminsky,Honeypot forensics part I: analyzing the network,IEEE Security & Privacy,Volume: 2, Issue: 4,Page(s): 72 –78, 2004.
[12] An Empirical Analysis of Phishing Blacklists, CEAS2009 Sixth Conference on Email and AntiSpam,July 16-17, 2009, Mountain View, California USA.
[13] Shujun Li,R.Schmitz, A novel anti-phishing framework based on honeypots,IEEE eCrime Researchers Summit, 2009.
[14] Michael ACaloyannides, Nasir Memon, Wietse Venema, Digital Forensics,IEEE Security & Privacy,Volume: 7, Issue: 2,Page(s): 16 –17, 2009.