International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

THE EMPIRICAL IMPLEMENTATIONS OF SECURED ALGORITHMIC APPROACHES IN ASSORTED NETWORKS

Amit Sharma
Assistant Professor
School of Information Technology
Apeejay Institute of Management Technical Campus
Jallandhar, Punjab, India

Dr. S.N.Panda
Professor and Principal
Regional Institute of Management and Technology
Mandi Gobindgarh, Punjab, India

Dr. Ashu Gupta
Assistant Professor
School of Information Technology
Apeejay Institute of Management Technical Campus
Jallandhar, Punjab, India

ABSTRACT

In the classical and most of the network attacks, the assailant injects enormous amount of junk packets into the network which leads to the thrashing of network resources and causes congestion among the wireless networks. The prevention mechanism divides into two categories - Local and Global. In the scenario of local solution, the protection of individual nodes involves three categories - local solutions, changing IPs and creating client bottle neck. By installing the filter on the local router to detect the infiltrating IP packets is stopped using time worn short term solutions. By changing the victims IP address is one of the techniques to prevent the attacker from accessing its network, however this technique is not effective, many attacker node will easily identify the newer IP address. The major objective behind this technique is creating bottleneck process on the zombie computers, for example making simple puzzle to solve before establishing connection or a software already installed in host computer asks to answer random question whenever attacker computer try to establish connection. The local solution consumes some time to perform connection this is unacceptable

drawback. Global solutions are meant for changing technology, there are three techniques to implement them including Improving entire internet security, Using global coordinate filters and Source IP address tracing. The classical technique is to prevent attacking nodes by collecting its time. If this filters are installed in internet, a host can send information about the attacker node that it has detected to the filter, the filter will stop attacking packets along with their path. This is one of the effective methods to prevent malicious threat. The main objective of this approach is to trace the intruder's path to the puzzle solving computers to stop their attack or to find the original attacker, and to take necessary action against it repeated attacks. However these techniques are not effective, because if the attacker node uses forged IP address, some of the hierarchical attacking structures hide the attacker from zombie computer. These are some major drawbacks. In the proposed scheme the fast forwarding and quick transferring problems are prevented by controlling the allocation vector, this technique increases Traffic on the network, Speed of data on nodes and Transmission time elapse. In this research paper, the empirical implementations have been performed for multiple networks in terms of security and integrity.

Keywords – Network Security, DDOS Attacks, Cloud Security, Cloud Server

INTRODUCTION TO THE DENIAL OF SERVICE (DOS) ATTACKS

In this type of attacks, the attacker injects enormous amount of junk packets into the network which leads to the loss of network resources and causes congestion among the wireless networks.

The prevention mechanism divides into two categories

- Local and
- Global

LOCAL SOLUTION : Protection of individual nodes involves three categories

- Local solutions
- Changing IPs
- Creating client bottle neck

LOCAL ROUTER SOLUTIONS : By installing the filter on the local router to detect the infiltrating IP packets is stopped using time worn short term solutions [1].

CHANGING IP ADDRESS : By changing the victims IP address is one of the techniques to prevent the attacker from accessing its network, however this technique is not effective, many attacker node will easily identify the newer IP address [2][3].

CREATING HOST BOTTLE NECK : The major objective behind this technique is creating bottle neck process on the zombie computers, for example making simple puzzle to solve before establishing connection or a software already installed in host computer asks to answer random question whenever attacker computer try to establish connection [4][5]. The local solution consumes some time to perform connection this is unacceptable drawback.

GLOBAL SOLUTIONS : Global solutions are meant for changing technology, there are three techniques to implement them

- Improving entire internet security
- Use global coordinate filters
- Source IP address tracing

IMPROVING ENTIRE INTERNET SECURITY : In this technique, all the computers linked to the internet are secured to prevent the attacker from attacking the host computer with some techniques like zombie.

USE GLOBAL COORDINATE FILTERS : This technique is to prevent attacking nodes by collecting its time. If this filters are installed in internet, a host can send information about the attacker node that it has detected to the filter, the filter will stop attacking packets along with their path. This is one of the effective methods to prevent malicious threat.

SOURCE IP ADDRESS TRACING : The main objective of this approach is to trace the intruder's path to the puzzle solving computers to stop their attack or to find the original attacker, and to take necessary action against it repeated attacks [6].

However these techniques are not effective, because if the attacker node uses forged IP address, some of the hierarchical attacking structures hide the attacker from zombie computer [7][8]. These are some major drawbacks.

In the proposed scheme the fast forwarding and quick transferring problems are prevented by controlling the allocation vector, this technique increases

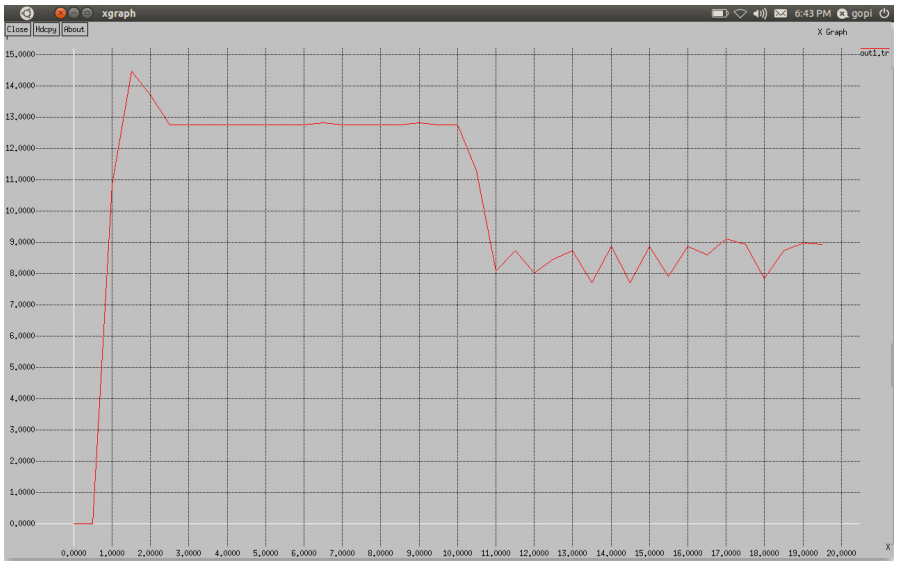
- Traffic on the network
- Speed of data on nodes
- Transmission time elapse

PSEUDOCODE DOS PREVENTION ALGORITHMS

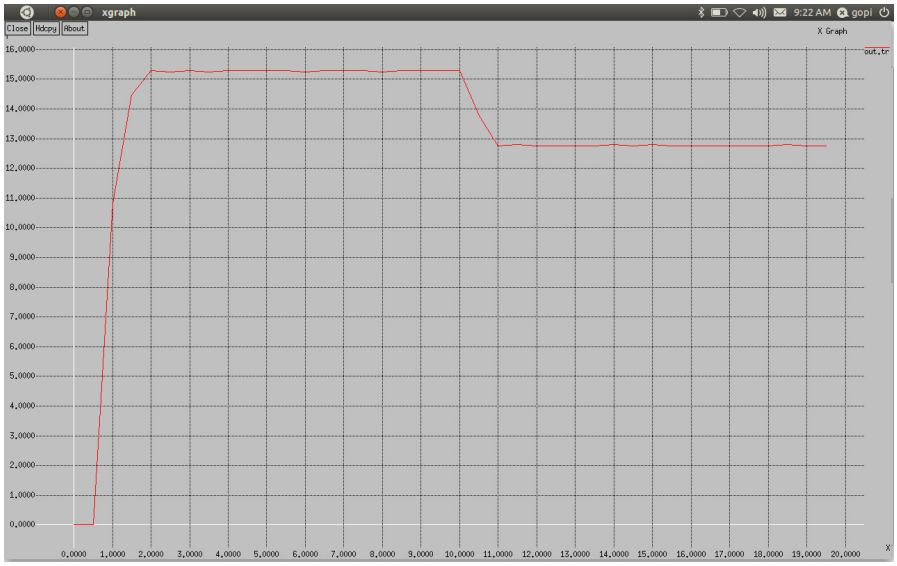
```
BEGIN
    Manage_constraint_check (node n, Data Unit d)
    FOR each p in n DO
        Manage_update (path p, Data Unit d)
    END FOR
END
```

POST IMPLEMENTATION GRAPHS

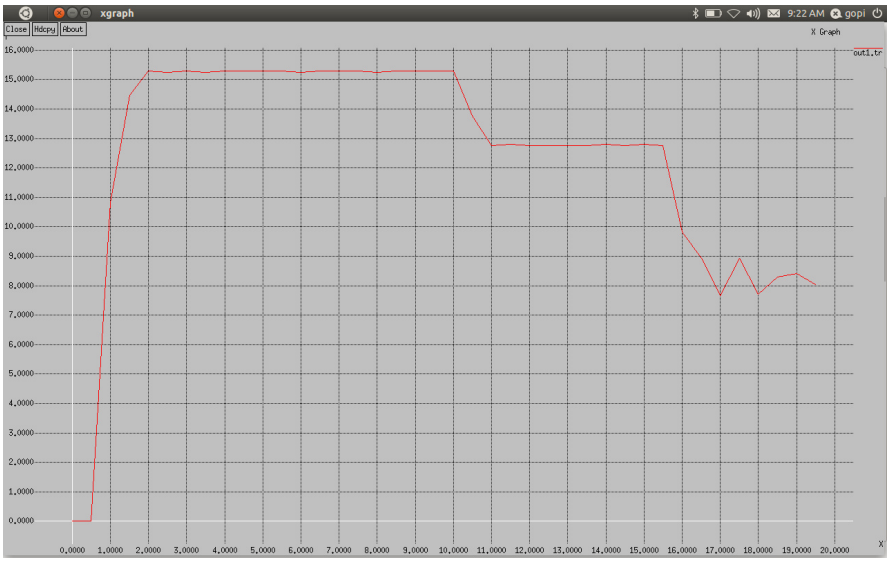
ATTACK THROUGHPUT



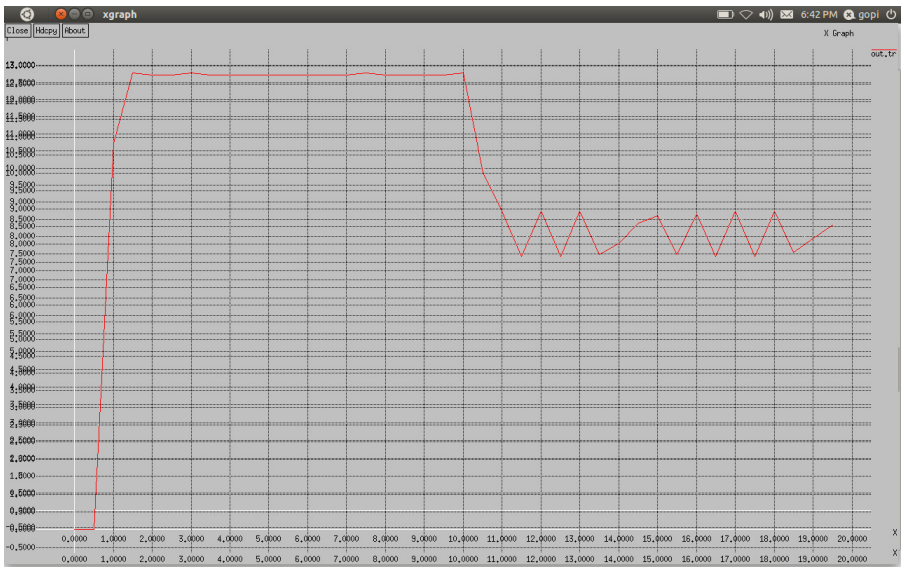
DELAY AFTER ATTACK



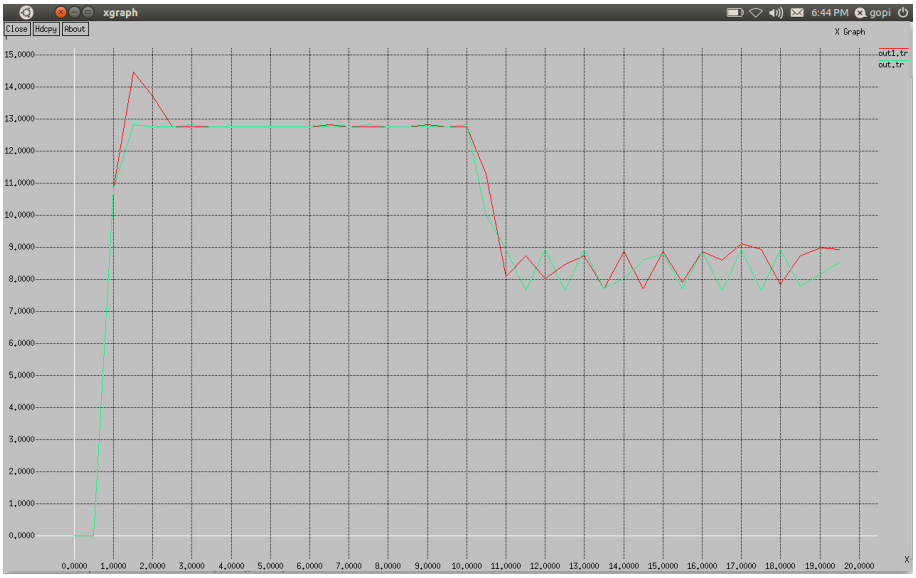
DELAY BEFORE ATTACK



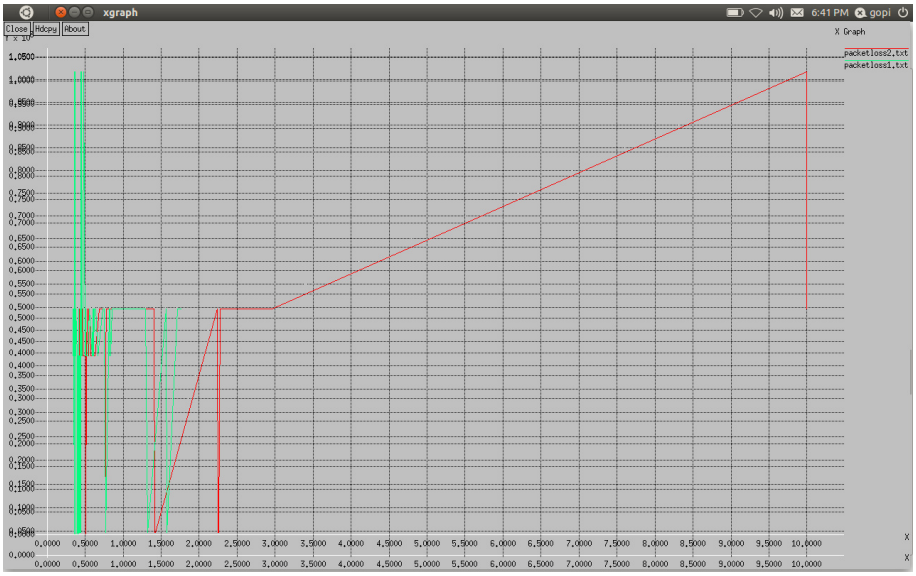
INITIAL THROUGHPUT



JITTER COMPARISON



PACKET LOSS COMPARISON



XGraph Types :

i)jitter=packets arriving in a particular node/time duration

ii)throughput=average packet delivered/time duration

iii)packetloss=number of packets dropped/time duration

iv)packet delay=similar to jitter.

v)for calculating jitter, throughtput, packetloss i used awk command to retrieve values.

NS2 CODE : Attackddos

```
#Open the new simulator
set ns [new Simulator]
set nf [open out1.nam w]
$ns namtrace-all $nf
#Open the output files
set f0 [open out1.tr w]
#$ns trace-all $f0
#Define a 'finish' procedure
```

```
proc finish {} {
        global ns nf f0 f
    $ns flush-trace
    close $nf
    exec nam out1.nam &
        #Close the output files
        close $f0
        #Call xgraph to display the results
        exec xgraph -x time -y throughput(mbps) out1.tr -geometry 800x400 &
#for the RED function
  global tchan_
  set awkCode {
        {
          if ($1 == "Q" && NF>2) {
                print $2, $3 >> "temp.q";
                set end $2
          }
          else if ($1 == "a" && NF>2)
          print $2, $3 >> "temp.a";
        }
  }
  set f [open temp.queue w]
  puts $f "TitleText: red"
  puts $f "Device: Postscript"
  if { [info exists tchan_] } {
        close $tchan_
```

```
    }
    exec rm -f temp.q temp.a
    exec touch temp.a temp.q
       exec awk $awkCode all.q
puts $f \"queue
    exec cat temp.q >@ $f
    puts $f \n\"ave_queue
    exec cat temp.a >@ $f
    close $f
    exec xgraph -bb -tk -x time -y queue temp.queue &
        exit 0
}
$ns rtproto DV
for {set i 0} {$i < 9} {incr i} {
set n($i) [$ns node]
}
$n(0) label "Server"
$n(1) label "Router"
$ftp6 attach-agent $tcp6
$ns at 15.5 "$ftp6 start"
$ns connect $tcp $sink
$ns connect $tcp1 $sink1
$ns connect $tcp2 $sink2
$ns connect $tcp3 $sink3
$ns connect $tcp4 $sink4
$ns connect $tcp5 $sink5
```

```
$ns connect $tcp6 $sink6



$ns color 1 Blue
$ns color 2 green
$ns color 3 Black
$ns color 4 green
$ns color 5 Black
$ns color 6 Red
$ns color 7 Red

#Define a procedure which periodically records the bandwidth received
proc record {} {
    global sink f0
        #Get an instance of the simulator
        set ns [Simulator instance]
        #Set the time after which the procedure should be called again
    set time 0.5
        #How many bytes have been received by the traffic sinks?
    set bw0 [$sink set bytes_]
        #Get the current time
    set now [$ns now]
        #Calculate the bandwidth (in MBit/s) and write it to the files
    puts $f0 "$now [expr $bw0/$time*8/261000]"
        #Reset the bytes_ values on the traffic sinks
    $sink set bytes_ 0
```

```
    #Re-schedule the procedure
  $ns at [expr $now+$time] "record"
}
```

MATHEMATICAL MODEL

$ATCK_i$ => ANZ ($ATCK_i$->SensNodesij) = > PEAij (PNF/FB/BL/ISE)=>S(SensNodesi)=>CR(ORi)

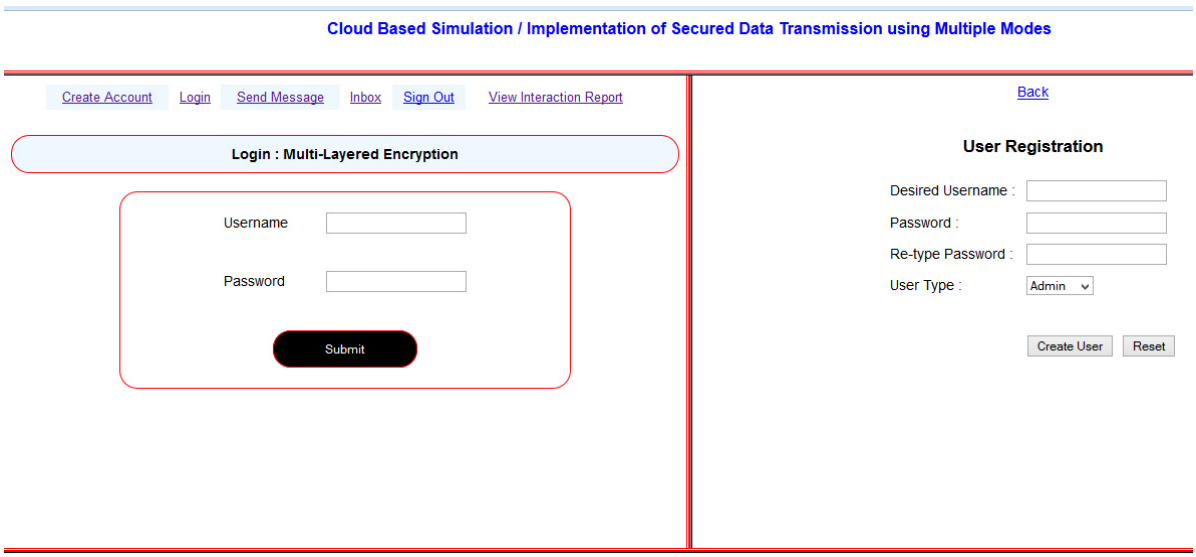
ATCK – $Attacker_i$

ANZ – Analysis Algorithmic Approach

PEA($SensNodes_{ij}$) - Performance Evaluation Algorithm on Sensor Nodes

CR – Cumulative Result

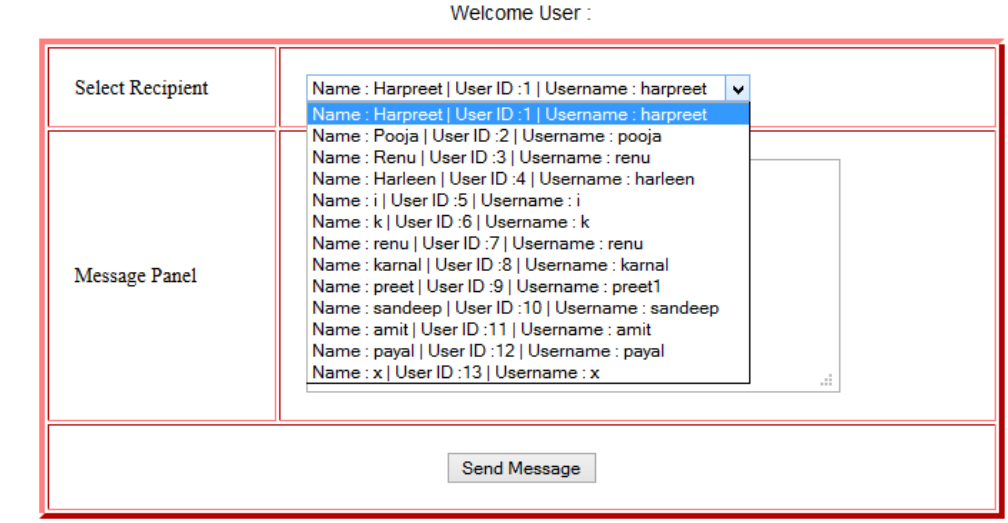
CLOUD SERVER SETUP WITH OUTPUT SCENARIOS



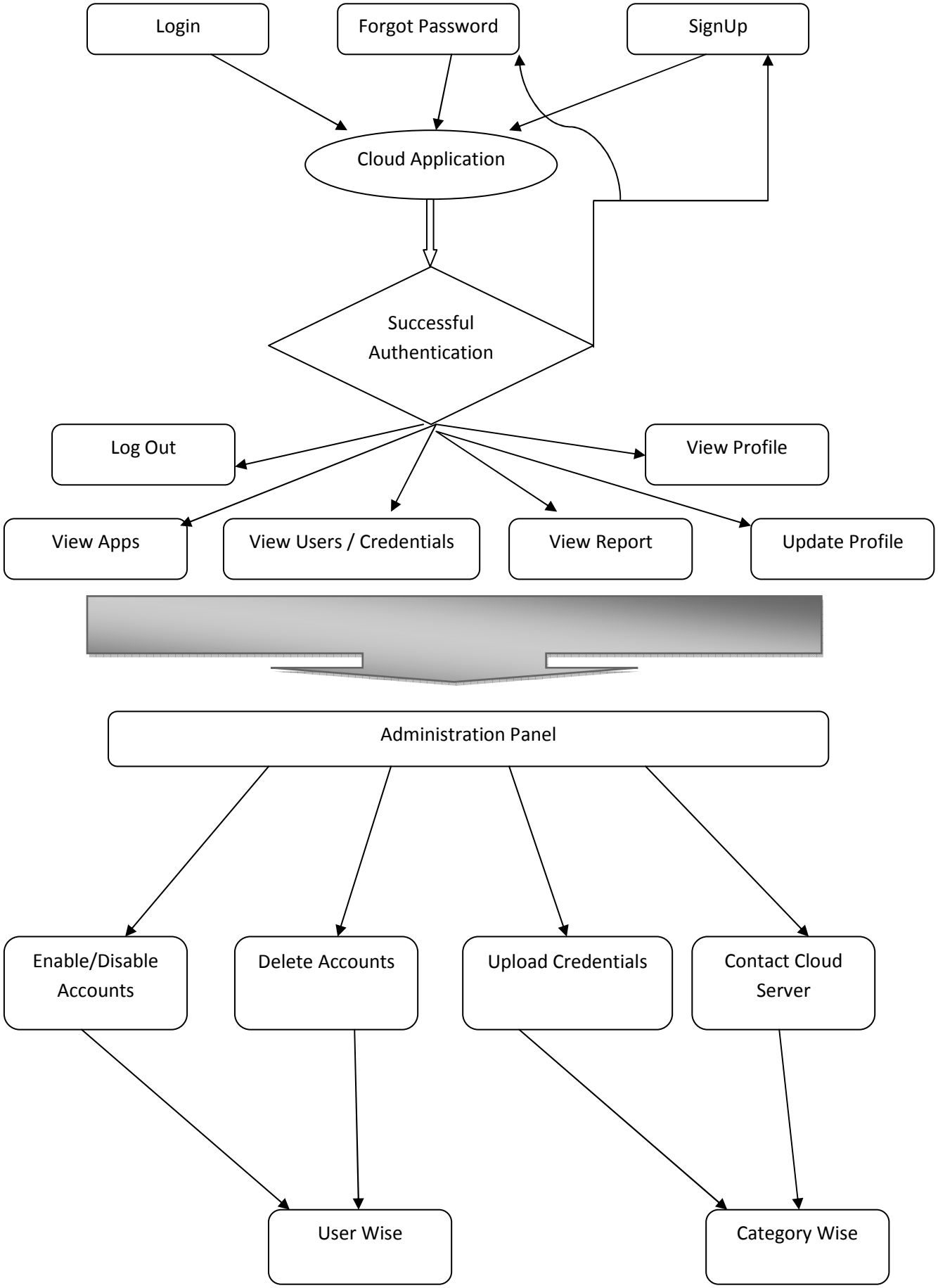
International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013



Sr. N.	Sender ID	Receiver ID	Message Transmitted	MD5 Hash Encryption	SHA1 Hash	Base 64 Encoding	Message Transmission Time (In Microseconds)	Date and Time
1	3	1	sdasadg	795571285282b603cdf89b66b5421179	59d001b1dca82f5c278bd6f81c683ce9c92c6181	c2Rhc2FkZw==	0.0012178421020508	May 25, 2012, 8:07 am
2	3	2		d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709		0.0025181770324707	May 25, 2012, 8:42 am
3	3	1		d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709		0.0012450218200684	May 25, 2012, 8:42 am
4	3	1	hello	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.001331090927124	May 25, 2012, 8:42 am
5	3	1	hello	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.001331090927124	May 25, 2012, 8:42 am
6	3	1	hello	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.001331090927124	May 25, 2012, 8:42 am
7	3	1	hello	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.001331090927124	May 25, 2012, 8:42 am
8	3	1	hello	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.001331090927124	May 25, 2012, 8:42 am


Login
Forgot Password
SignUp
Cloud Application
Successful Authentication
Log Out
View Profile
View Apps
View Users / Credentials
View Report
Update Profile
Administration Panel
Enable/Disable Accounts
Delete Accounts
Upload Credentials
Contact Cloud Server
User Wise
Category Wise

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

Cloud Data Transfer Mathematical Model

CU (Cloud User) -> RGN (Registration) : (CS : Cloud Server)

-> DCS (Admin. Decision)

-> Y (Approval)

-> DPT(Data Packet Transmit)

-> SR (Select Authenticated Recipient) -> IDT (Initiate Data Transfer)

(SMO) -> Secured Mode On for Encrypted Data Transmission

(MDET) -> Multiple Data Encryption Based Transfer

-> CIM (Check Incoming Messages)

-> N (Denial)

-> RFA (Request For Approval)

-> PG (Permission Granted) -> IDT (Initiate Data Transfer)

(SMO) -> Secured Mode On for Encrypted Data Transmission

(MDET) -> Multiple Data Encryption Based Transfer

REFERENCES

[1] T.H Clausen, “Introduction to Mobile Ad-hoc Networks (MANET)”, 2007.

[2] Che-Fn Yu, “Security safe guards for intelligent networks”, GTE laboratories incorporated, 40 sylvan road, Waltham, MA 02254.

[3] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, "WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, IEEE, 2008.

[4] Tuna Guven, Hui Zeng, Jason H. Li, Song Luo, Subir Das, Tony McAuley, Thomas Stuhrmann, Joe Sherrick, Christine Adelfio, Seth Spoenlein, Aristides Staikos, Mario Gerla, "A Multi-Layer Approach For Seamless Handoff In Ad Hoc Networks With Wireless Heterogenity", IEEE, Paper ID 900668.pdf.

[5] S. Prasad, Y.P.Singh, and C.S.Rai, " Swarm Based Intelligent Routing for MANETs", International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009.

[6] Poonam Garg, "A Comparison between Memetic algorithm and Genetic algorithm for the cryptanalysis of Simplified Data Encryption Standard algorithm", International Journal of Network Security & Its Applications (IJNSA), Vol.1, No 1, April 2009

[7] Jason Leonard, "Interactive Game Scheduling With Genetic Algorithms", 1998

[8] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", international conference on wireless networks, 2003