Honeypots: Screening Cyber Attacks

Adnaan Arbaaz Ahmed
Director,
Techionary,
Dilsuknagar, Hyderabad

Vanam Rajkumar
CEO,
Techionary
Dilsuknagar, Hyderabad

M. I. Thariq Hussan, PhD
Prof & Head,
Department of Information Technology, GNITC,
Ibrahimpatnam, Hyderabad

ABSTRACT
Cyber attacks have been a part of modern human combat. Various technologies like Intrusion detection system (IDS), Intrusion Prevention system (IPS), firewalls are under active monitoring to generate alerts and in preventing cyber-attacks. However, these mechanisms are not the solutions as they cannot generate accurate solutions, potentially Intrusion detection system tend to generate false signals. Perhaps, cyber attacks cannot be just controlled with just tools. Instead it requires an Indicator of compromise (IoC) which is an important subject in IT sector to identify true positive attacks. In this paper, it is proposed a new threat intelligence technique which evaluates by analysing honeypot's log data to identify true cyber attacks and to immediately act anincident response process. This goal is achieved by deploying a honeypot on an AWS cloud to gather cyber-attacks. This method of malware bypasses technical solutions by leveraging social engineering methods in order to prevent ransomware attacks. An additional system for perimeter defence is established. Honeypots are spurious computer resources deployed by network administrator to act as decoy computers and identify any informal access. Investigations determined a suitable method to identify changes to this aspect. Two options were filed under research, one is the file screening service of the Microsoft File Server Resource Manager feature and the other is Event Sentry to manipulate the Windows Security logs. Under development process, a determined response to attacks to the system along with threshold were initiated. The research also mentioned that witness to tripwire files offered limited value as there is no alternative to influence the malware to access monitored files.

General Terms
Your general terms must be any term which can be used for general classification of the submitted material such as Pattern Recognition, Security, Algorithms et. al.

Keywords
AdbHoney, Amun, Artilliary, AWS, CiscoASA, Cowrie, Conpot, Cyber Attacks, Cyber Security, Dianaea, EC2, Elastic Pot, Elastic Search, Glastopf, Glutton, Heralding, Honeypie, Honeypots, Honeytrap, Kibana, Kippo, LogStash, Mailoney, P0f Engineering tool, Port Forwarding, Port Numbers, Rpdy, Security, Server logs, Snare, Tanner

1. INTRODUCTION
Honeypot is a program or a server which is made voluntarily vulnerable to attract and capture hackers. The attackers who think they have targeted a real resource using their attack techniques and tools against the probed site, allows the defender to observe and monitor the activities of the hacker and analyse their attacking methodologies which are used to learn and prepare a defence mechanism for the real resources. An old idiom says "more flies are caught with a drop of honey than a bowl of vinegar" which suits our topic specifically, honeypots are precisely attracting attacks to frame an idea about the attacker. We may wonder "who is going to attack me if I belong to a small business, a not so important guy on the internet?" In reality, threats are automated programs which are engaged in the cyber environment, surfing victims through webcams, refrigerators, television, routers and many devices. For example, denial-of-service which is used in attacking a web domain or to keep a record and sneak into all the data that comes in its way.

2. TYPES OF HONEYPOT
Based on deployment and involvement, honeypots can be classified as

i. Production honeypots
ii. Research Honeypots

Production Honeypots function with ease to capture limited data which are essentially used by companies. Production honeypots are nested within a production network along with organisation's production server to improve security. In other words, production honeypots are easy to deploy and they give meagre information about the attacks when compared to research honeypots

Research Honeypots are deployed to collect information about the moves and tactics of the Blackhat community whose target are different network. Research honeypots have an indirect value to its organisation; besides, they are used to study the threats and learn to counter them. Research honeypots are complex to maintain and deploy. These are preferred by research, military or government organisations

Based upon Design criteria, Honeypots can be classified as follows

i. Low-interaction honeypots
ii. Medium-interaction honeypots
iii. High-interaction honeypots

Low-interaction honeypots function only the frequent services which are requested bt attacker. Multiple virtual machines can be hosted on one physical system as it consumes relatively less resources. These virtual systems have a short response time and fewer lines of code is required which reduces the complexity of the security.

Low-interaction honeypots depict the hacker emulated service with a limited subset of functions which they expect from a server. Keeping in mind of detecting sources of unauthorised functions. For instance, a HTTP service on low-interaction honeypots supports only commands which are used to identify that a authorised request is attempted.

Medium-interaction honeypots are fully deployed in the HTTP protocol suite to an authorised implementation like Apache. Inspite, there are no medium-interaction honeypots

discussed in this paper. Low-interaction honeypots captures medium interaction honeypot's functions in a way that only provide specific implementation of service and doesn't allow typically, full interaction honeypots with the system.

High-interaction honeypot resemble the actins of a real system that is a host of variety of services. It allows the hacker interact with the system as an operating system does, with the intention of capturing full potential information on the attacker's technique. Commands or application wherein the end user would install is available. There are no limits to hackers for his actions to compromise on the system. Research study claims that high-interaction provide full length security by being difficult to detect, but with a limitation for each physical computer which can lead to increase in cost like honeynet.

3. FLAVOURS OF HONEYPOT

3.1 AdbHoney

the Android Debug Bridge which is a protocol framed to track emulated and real phones which are connected to their host. Implementation of commands aid the developer which is usually done via USB cable with ample mechanism of authenticity and security, which turns out by a simple ADB command viz, (adbtcpip<port num>) sent to establish connection. A device can be forced to expose its services over 5555 port, later a simple adb connect<ip>:<port num> to connect to the device over TCP. Unlike USB protocol, TCP one does not have authentication and leaves the device prone to attacks.

3.2 CiscoASA

Cisco Adaptive Security Appliance is a software which is the centre of an operating system that powrs the cisco ASA family. CiscoASA delivers enterprise-class firewall functions for ASA devices in an array of form factor like standalone applications, virtual and blades. ASA integrated with critical security technologies to deliver comprehensive solutions to meet evolving needs in security.

CiscoASA benefits:

i. Integrated IPS, VPN and Unified Communication capabilities

ii. Increasing capacity and enhance performance of organisation by means of clustering

iii. Delivering high availability for high resiliency applications

iv. Providing awareness in context with cisco trust security group and Identity based firewall

v. Promotes dynamic routing and VPN for site-to-site on a pre-context basis

vi. Besides the functionality of a firewall, CiscoASA can also act as:

   a. Antivirus

   b. IDS/IPS engine

   c. SSL device

   d. Antispam

   e. Content inspection

3.3 Conpot

It is an ICS honeypot with the intention of collecting information about the motive and methods of attacks focused to Industrial Control system. In addition, Conpot has a low-interaction on server side control system framed to be simple to for deployment, modification and extension. With a range of common industrial control protocols, basics to build required system which is capable of emulating complex infrastructures to convince an attack is designed along with methods to improve deceptive capabilities possibility for server with a custom human machine interface to increase attack is made possible in this research.

3.4 Cowrie

It is a medium to high interaction Secure shell and telnet honeypot framed to log brute force attacks and the shell interaction performed by the attacker. It performs a UNIX system in python when on a medium-interaction mode, in high-interaction mode, it functions as an SSH and Telnet proxy to track attacker's behaviour

3.5 Elastic pot

It is a honeypot scripted in python 3.5 version. It functions GET PUT, POST, DELETE requests with backend as yes elastic

3.6 Glutton

It is an "all eating honeypot" scripted in GO language which acts as a proxy between attacker and other honeypots with a facility to capture log and analyse the request sent. It sneaks to all the ports and then function to a protocol file or rule file.

3.7 Heralding

It is a low-interaction honeypot which will allow user to emulate various protocol with a user interface. On the attack is taken place all the details will be noted in log file.Protocolslikepop3,http,https,imap,imaps,vnc,smtp,stocks5 and PostgreSQL are supported

3.8 Honeypie

It is designed to attempt a reliable indicator of compromise with less to no setup charges. It only flags that would trap many attackers in a network

i. Port Scanning Activities

ii. FTP Connection Attempts

iii. Telnet Connection Attempts

iv. VNC Connection Attempts

3.9 Honeytrap

Honeytrap is an opensource honeypot with a variety of modes which can be used to deploy complex honeypot architecture

3.10 Mailoney

It is a SMTP based honeypot which are various in modules that facilitates custom modes to fit user's needs.

3.11 Rdpy

Remote Desktop protocol in twisted python is an implementation of python of Microsoft Remote desktop protocol supporting client and server side. It is deployed bovver the event driven network engine. It supports standard RDP security layer.

Rdpy provides binary like

RDP Man In The Middle proxy which record session

i. RDP Honeypot

ii. RDP screenshoter

iii. RDP client

iv. VNC client

v. VNC screenshoter

vi. RSS Player

3.12 SNARE

Super Next Generation Advanced Reactive Honeypot is a web based honeypot which has similar features of Glastopf to rewrite existing web pages into attack surface with Tanner.

3.13 Tanner

In general the SNARE's brain is termed as Tanner. Tanner decides every event sent from snare with a respond to client. This allows in changing behaviour of many sensors on the fly.

4. PROPOSED SYSTEM

Server logs are examined by security professionals after the attack is made to get the IP address of the attacker to ensure that any attacker is to get credentials and maintain it in the server. If the IP address is changed by spoofing the IP with VPN's or TOR network it will create a hectic situation for any cyber expert to trace the attacker, which leads to the deface of network by the attacker.

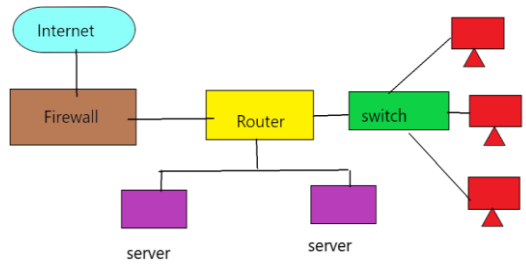

Fig 1: block diagram of existing approach for cyber investigation

Here in the proposed model on honeypots to automate the process of tracking the attackers even without viewing the logs of the server, honeypots are deployed in the network to trap the attacker.

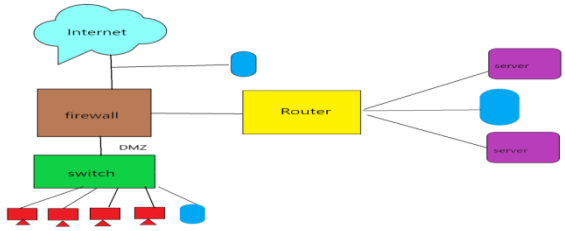

Fig 2: Block diagram of proposed methodology for cyber investigation

4.1 System Architecture

A server operating with a honeypot is deployed on the EC2 instance of AWS cloud and in the security group, the inbound rules will be open from port 0 to 65535 from anywhere i.e 0.0.0.0/0 . the inbound rules are changes as figured below

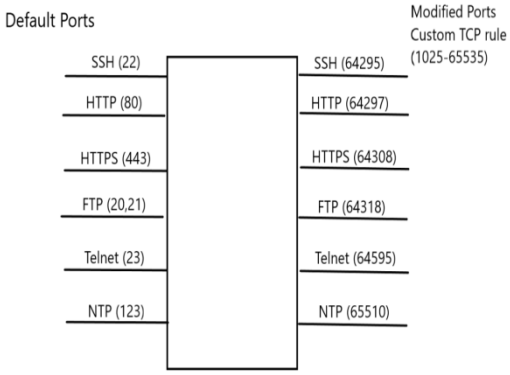

Fig 3: System Architecture

The default ports of access are modified to our customised ports. The original data of the server is forwarded to our customised ports. The attacker trying to access the server with the default port numbers will be alarmed as unauthorised person. In the default port numbers, fake data is kept to mislead the attacker. Here honeypot acts as a decoy computer for storiing fake data of the server and it records the IP address of the attacker and blocks the access to the network.

4.2 Implementation

Step 1: Creating an EC2 instance on AWS cloud.

Step 2: Deploying Dianaea, Kippo, Amun, Artillery, Glastopf, ElasticSearch, Log Stash, Kibana honeypots on the EC2 instance.

Step 3: Changing the Security Group inbound rules.

Step 4: Enabling port-forwarding in the server.

Step 5: Storing the bogus information on the honeypot server.

Step 6: Installing the p0f fingerprinting tool for extracting the data of the attacker.

Step 6: Testing the created environment.

Step 7: Analysing the results.

4.3 Results

The data collected from all the honeypots for a period of 6 months. All the data published as results is collected by the p0f tool.

4.3.1 P0f fingerprinting tool

P0f is a multifaceted passive Operating System fingerprinting tool which can identify the system of machines that connect your instance and even the machines merely go through or near your instance even if the machine is behind the packet firewall. P0f records the logs of the user accessing the system. And we have used the logs of p0f to extract the following information about the attacker.

4.3.2 Operating system

A comparison of attacker Operating Systems can be seen in Figure. The honeypots in EC2 received roughly the same number of attacks from Linux-based attackers as Windows-based attackers. Our Azure instances received roughly 50% more attacks from Windows-based attackers.

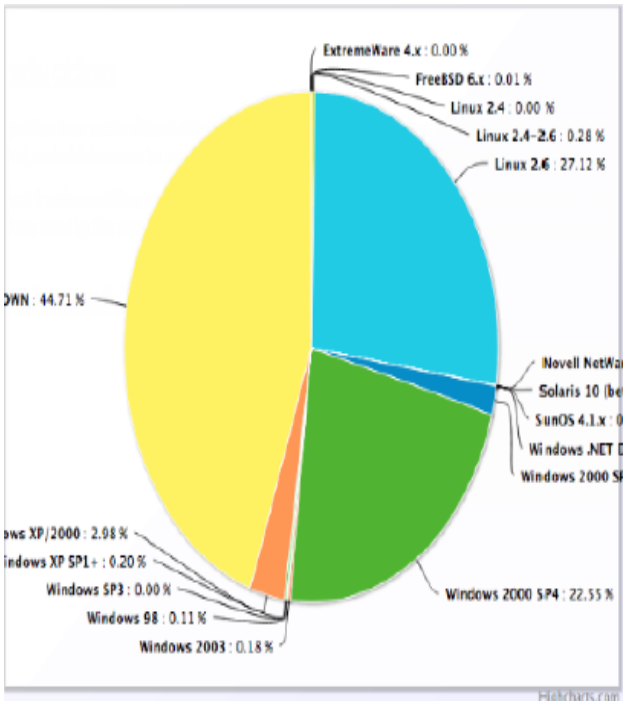

Fig 4: attackers operating system

4.3.3 *Geographic location*

The top countries from which attacks originated were listed out in the figure. As we can see that most of the attacks form China, United States, Russia, followed by Taiwan, Brazil and Romania.

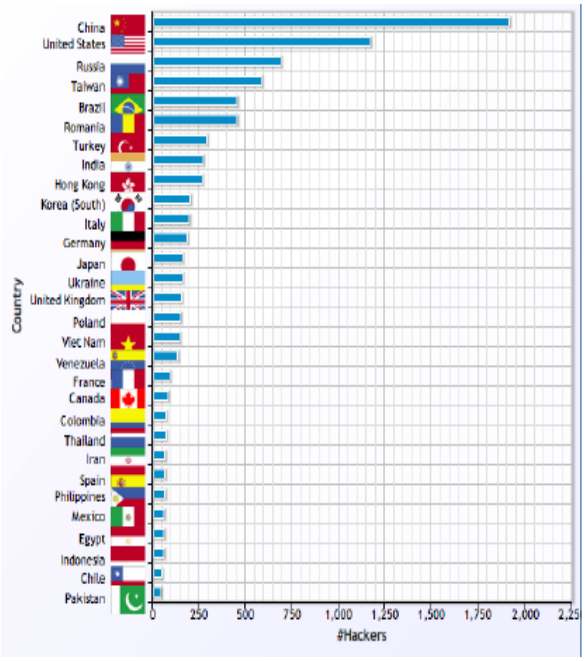

Fig 5: Attacks by the country (top 30)

4.3.4 *IP addresses*

Additionally, our instances were able to isolate a handful of IP addresses that are responsible for thousands of connection attempts as listed below

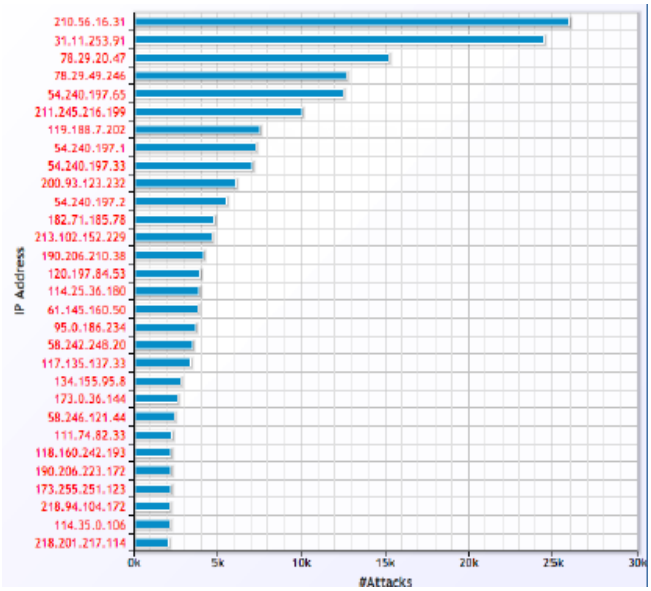

Fig 6: top 30 attackers IP address

4.3.5 *SSH login credentials*

Our instances faced thousands of automated SSH brute force attacks. The most common username was “root". Other usernames such as \sa" and \mysql" were attempted, but to a far lesser extent. As for passwords, attackers most commonly tried the empty sting (“"), “123456", and “password". Attackers also tried variations of common passwords that users and easy to type such as “qwerty" and “1qaz2wsx." The results from EC2 can be seen in Figure

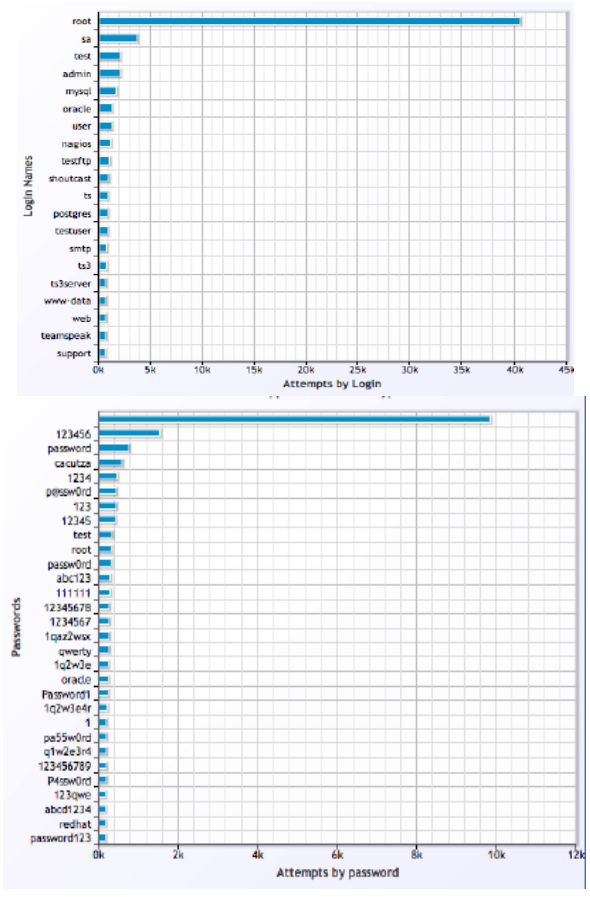

Fig 7: top 20 SSH login credentials

Fig 8: Log Stash of Kibana

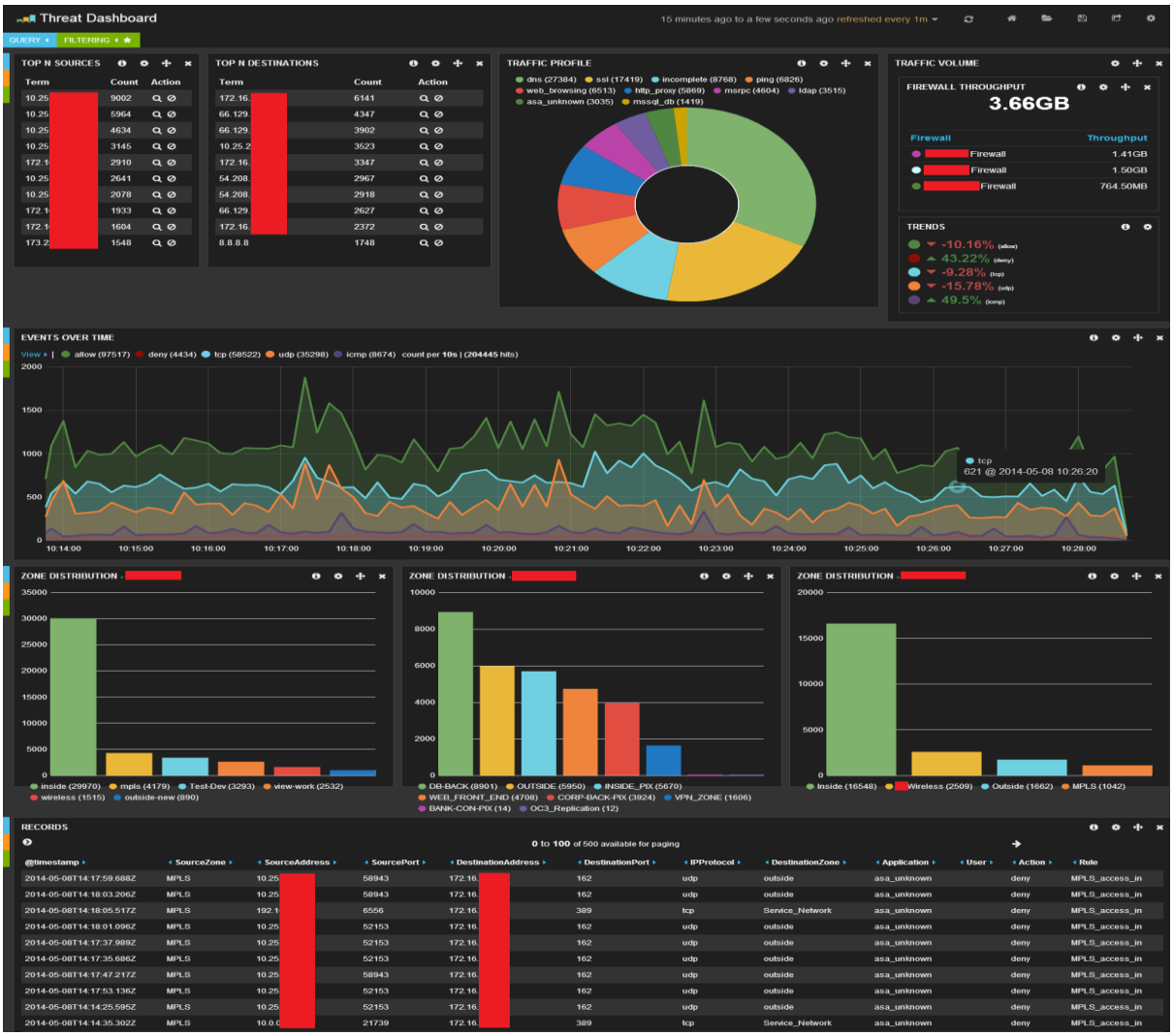

Fig 9: Network operations with ELK (Elasticsearch, Log stash, Kibana)

5. ACKNOWLWDGEMENT

In our study we were able to determine a basic attacker profile by deploying a variety of honeypots in AWS cloud. We found that attacks mostly come from China and the US. The most commonly attempted user was \root" and most commonly attempted passwords were \" and \123456". The services that were targeted most frequently were SSH and HTTP. In terms of OS, Linux 2.6 and Windows 2000/XP were the most popular, and ethernet/modem was the connection protocol used the most. The timing of attacks was very random and bursty across all the regions and we could not identify any particular time of the day when hackers are most active.

We were also able to identify the honeypots which are most effective in the cloud setting. Dionaea and Kippo, Kibana performed very well and produced copious amounts of useful data. The other honeypots Amun, Artillery and Glastopf were not as effective, given that they received little traffic beyond port scans.

6. REFERENCES

[1] AdnaanArbaaz Ahmed, Dr. M.I. ThariqHussan, "Cloud Computing: Study of Security Issues and Research Challenges", International Journal for Advanced Research in Computer Engineering and Technology Volume 7, Issue 4, 362-369, April 2018.

[2] AdnaanArbaaz Ahmed, Durganath Rajesh, Dr. M.I. ThariqHussan, "Implementing Machine Learning Techniques in Malware Detection", International Journal for Research in Engineering Application and Management Volume 4, Issue 9, 155-158, December 2018.

[3] AdnaanArbaaz Ahmed, Dr. M.I. ThariqHussan, VenkateswarluBollapalli,"Upgrade- Data Security in Cloud by Machine Learning and Cryptography Techniques", International Journal of Engineering and Advanced Technology Volume 8, Issue 6, 2728-2732, August 2019.

[4] Navneet Kambow , Lavleen Kaur Passi, "Honeypots: The Need of Network Security" International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6098-6101

[5] Pavol Sakol, Jakub Misek, Martin Husak, "Honeypots and honeynets: issues of privacy" EURASIP Journal on Information Security, February 2017

7. AUTHORS PROFILE

Adnaan Arbaaz Ahmed popularly known as Technophyle Ahmed is a tech junkie and a self proclaimed offensive and defensive ethical hacker and security expert of computer systems. He is specialized in Networking, Cloud Computing, Linux, Java, Python, Ethical Hacking, Cyber Security, Machine Learning, Artificial Intelligence, DevOps, Data Science, Containers Technology, Blockchain, etc. He is the director of Techionary. He delivered almost a 50 workshops on the above listed domains igniting young minds with advancements in Technology. He has four international publication out of which two are industrially implemented. Life time member of World Research Council. Honored with the title Research Ratna 2019 as the Best Researcher in Information Technology by RULA Awards.

Vanam Rajkumar, is the Chief of Executive of Techionary. Speaker for Institute for Engineering research and Artificial Intelligence (IERAI-2020) for the topic "AI assisted chatbot for visually impaired and disabled persons" . Member of International Association of Engineers society of Artificial Intelligence (IAENG). Project fellow at Foundation for Advancements In Engineering and Research (FAER-2019) for the proposal titled "Detection of harmful gas to ensure safety and security of human life and property."

Dr. M.I.Thariq Hussan has 18 International and 1 National journal publications. He has presented papers in 31 International/National conferences and attended 36 Seminars/Workshops/FDP/QIP. He has published 2 books titled 'System Analysis and Design' and 'Operating Systems'. He has received 'Innovative Technological Research (Communication) and Dedicated Professor Award' from Innovative Scientific Research Professional Malaysia (India Chapter). He also received 'Best Teacher Award-2018' from Institute for Exploring Advances in Engineering accredited by EA-JAS. He has filed 2 patents titled 'Vision Based Safety Seat Belt Monitoring System' and 'Intelligent Detect and Control Cybercrime Device'. He has qualified ESOL certificate in English by Cambridge University. He is a life member of ISTE and nominee member of CSI for knowledge exchange and enhancement.