Detection and Control of Malicious activity and Digital Forensic in BYOD

Md Iman Ali, Sukhkirandeep Kaur

Abstract: Enterprises are focusing greatly on Bring your own Device strategy since 2009 when Intel Adopted Bring your Own Device phenomena for the employees and later on this became more popular, Since 2012 exponential growth of BYOD services in the corporate environment also observed for providing an alternate method of working environment using employee personal device, however due to increased security threats and malicious activities occurring in BYOD environment most of the corporate are facing major challenges in enabling BYOD program. Increased Cyber-attack fragmenting the business ecosystem and cyber security becomes business survival factor. Increased amount of cyber attack in BYOD environment has created a major road block in adoption of BYOD. Existing security models of BYOD implementation, tools and techniques does not match the pace of security landscape at which cyber threats are growing. Moreover existing detection and control techniques of malicious activities in BYOD environment are not sufficient for cyber forensic investigation post an attack. By creating a secured model of BYOD environment security risk can be reduced. During this research Two different approach was followed to mitigate these risks. First approach was reverse adoption of encryption technique used to protect corporate network from BYOD environment. In 2nd approach malicious activity detection and protection mechanism explored with cyber forensic readiness in BYOD environment. Significant positive result observed to protect the corporate network infrastructure from untrusted BYOD traffic using GetVpn in cluster deployment. 2nd phase of this research has resultant to build digital forensic readiness BYOD model. Building a cyber secured model of BYOD cluster deployment ecosystem has contributed to reduce the risk of cyber threat. And detection of malicious activities has contributed in building a cyber forensic BYOD infrastructure to provide cyber confidence BYOD services.

Keywords: Cyber Security, Digital Forensic, BYOD, Encryption.

I. INTRODUCTION

Bring your own device (BYOD) is connecting non trusted external devices in Corporate network infrastructure. Creating alternate method of working model to increase employee productivity and employee satisfaction strategy project running almost majority of the organization. Predicted adoption of BYOD services by 2022[1] are expected to increased by 75% as per the study conducted by Gartner from 35% in 2018 which is almost double of the growth. By 2021[2] maximum organizations are expected to use IoT, 94% of the organization will adopt IoT as per Microsoft report. This pace of growth are also reason for increasing the cyber security risk and data leakage incident. Unmanaged devices might not be following the standard security practice, may not follow line of defense against

malicious content[3]. Risk of malicious activities are also increased in BYOD environment as the devices increased.

A Study concluded 62% of digital incidents are triggered by inside users either by intention or by unintentional [4]. Md

Securing BYOD infrastructure by using multiple tools and technique always been explored but due to increased amount of threat landscape and advancement of threat tools and techniques always there is a need of advancement of further research.

1.1 PREVIOUS STUDY:

1.1.A CERTIFICATE BASED SECURED AUTHENTICATION MODEL : Certificate based Hybrid authentication model with 3 tier captcha collective model of authentication was one of the successful model[5]. Secured authentication model of framework was explored for secured authentication and onboarding of BYOD internal users[6].Also dual factor authentication method has been analyzed for secure communication. using Scyther Tool and computerized dual factor authentication mechanism is tested for automatic verification tool with secured approach in IoT[7]. Secured model of authentication with 802.1x authentication was explored implementing network security control[8]..

1.1.B BYOD ENCRYPTION SECURITY MODEL: Encryption technology is used to encrypt corporate data in mobile devices[9]. Encryption/cryptographic method of network security is an option in a recent research in 2019 explored end to end encryption is secured model [10]. Denial-of-Service Attack (DDoS) attack in remote access connection and network traffic gets congested remote site traffic authentication traversing is a challenge[11] and explored IDS/IPS are essential components studied.

1.1.C BYOD BLOCK CHAIN AUTHENTICATION: Advance level BYOD block chain technique authentication with self service portal was explored where authentication process reduce the risk of data leakage and threat due to unauthorized access and thus secured the core network infrastructure from attack[12]. Multi factor block chain secured model of block chain cryptographic authentication model was explored for building enhanced secured BYOD environment[13].

In a cluster deployment of BYDO environment pre-authentication traffic traverse through corporate MPLS network where corporate network and BYOD network converge to reach the destination for authentication server. In this scenario there is a major risk of security breach.

Manuscript published on November 30, 2019.
* Correspondence Author

Iman Ali*, Research scholar, Department of computer application, Lovely Professional University, Punjab, India

Dr Sukhkirandeep Kaur, Assistant Professor in Department of Computer Science and Engineering, Lovely Professional University, Phagwara

First objective of this research is to secure the corporate network from BYOD traffic while traversing through same corporate network using reverse adoption of BYOD traffic encryption.In our 2nd approach post authentication of BYOD users detection of malicious activities are examined and control mechanism is explored.

Second objective of the research is to detect the malicious activities and enable a control mechanism to protect the BYOD infrastructure and corporate network.

II. DESIGN AND IMPLEMENTATION METHODOLOGY

During the research we have explored 2 different approach for securing Network and malicious activity detection for forensic investigation

In first approach corporate network infrastructure is protect from BYOD untrusted network.

2nd approach was taken for detection of malicious activities and protection mechanism was analyzed.

2.1 BYOD AUTHENTICATION TRAFFIC ENCRIPTION TO REDUCE CYBER RISK

Traffic encryption [14]was used as first level of mitigation[15] to reduce cyber threat risk. Authentication traffic from branch location to central location is encrypted using Get VPN to secured the communication between branch untrusted BYOD traffic to central location authentication destination, Get VPN was used to secure the traffic over MPLS [16] which encrypt the communication and protect the internal network from threat[17] to reduce the attack from BYOD users.

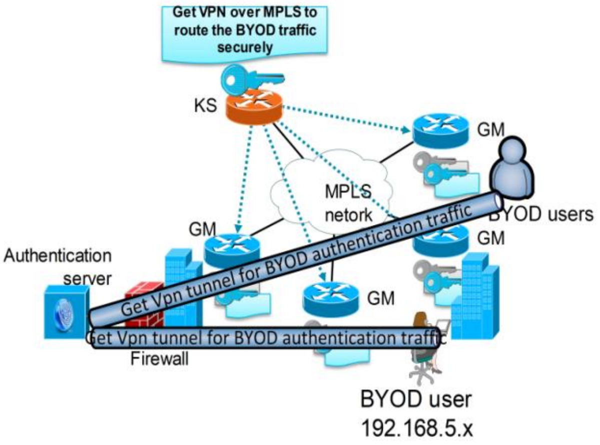

Get VPN over MPLS to route the BYOD traffic securely
KS
GM
MPLS netork
GM
BYOD users
GM
Authentication server
GM
Get Vpn tunnel for BYOD authentication traffic
Get Vpn tunnel for BYOD authentication traffic
Firewall
BYOD user 192.168.5.x

Figure 1: BYOD Authentication untrusted traffic over MPLS using Getvpn.

Additional components used for this testing for authentication traffic between branch location to central location

Table 1: components for BYOD traffic

Sl.no	Components	Purpose
1.	MPLS connectivity	Authentication traffic flow between branch and central location.
2.	Internet link	Local exit for BYOD internet traffic.

IP address used during the test for pr-auth and post auth traffic[6] as per solution of “BYOD Secured Framework”

Table 2: IP address schema

Sl No	Pre-auth subnet	Post-Auth subnet	Note
1	192.168.x.x/16	172.28.x.x/16	Segmented IP address used for major subnet

Initial authentication traffic was routed from Branch location to Central location encrypted using Getvpn. Implementation of getvpn was done as per standard guideline[16].

Encryption acl configured on Getvpn Key server as below

Table 2.1: Encryption policy on Key server

Getvpn-Keyserver#show crypto gdoi ks acl
Group Name: BYOD-Test
Configured ACL:
access-list LAN deny udp any any port = 848
access-list LAN deny udp any port = 848 any
access-list LAN deny tcp any any port = 179
access-list LAN deny tcp any port = 179 any
access-list LAN permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

In the policy 192.168.x.x network is encrypted for traversing through corporate MPLS network along with corporate trusted IP segment. Policy configured on Key server for encryption of BYOD traffic over MPLS for Group member

Table 3: Getvpn GDOI security policy

Getvpn-Keyserver#show crypto gdoi ks policy
Key Server Policy:
For group GETVPN-Test (handle: 2147483650) server 10.1.1.1 (handle: 2147483650):
of teks : 1 Seq num : 6
KEK POLICY (transport type : Unicast) spi : 0xC68CC7816905D0DA41A7DF6A218D6A0A
management alg : disabled encrypt alg : 3DES
crypto iv length : 8 key size : 24
orig life(sec): 86400 remaining life(sec): 66918
sig hash algorithm : enabled sig key length : 294
sig size : 256
sig key name : HO-KS-KEY
TEK POLICY (encaps : ENCAPS_TUNNEL)
spi : 0x80B694D2
access-list : BYOD
transform : esp-aes esp-sha-hmac
alg key size : 16
sig key size : 20
orig life(sec) : 3600 remaining life(sec) : 2624
tek life(sec) : 3600
elapsed time(sec) : 976
override life (sec): 0
antireplay window size: 64
For group GETVPN-Test (handle: 2147483650) server 10.1.1.2 (handle: 2147483651):

As shown above BYOD traffic is encrypted and encapsulated with TEK Policy. During the research BYOD environment was setup using multiple hardware/equipment. Design of BYOD with Getvpn for Guest traffic simulated in this research was as show below.

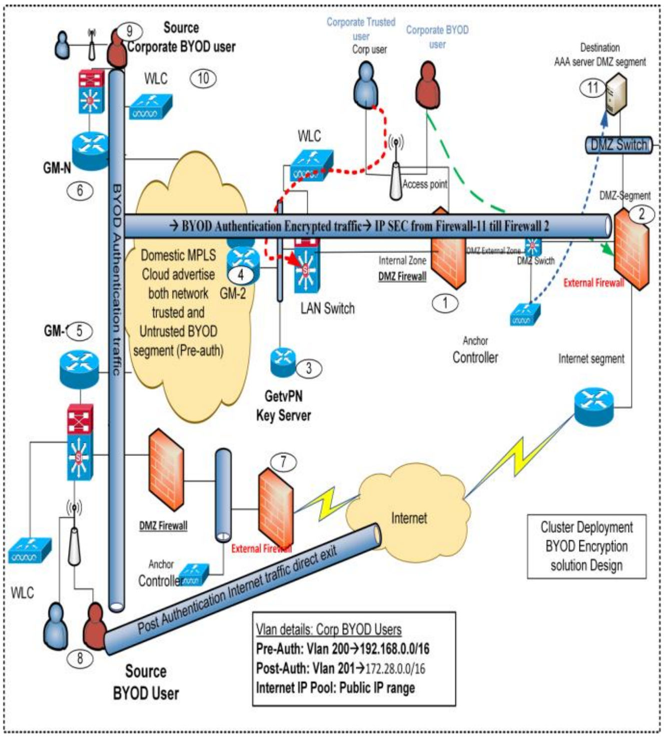

9
Source
Corporate BYOD user
WLC
10
Corporate Trusted user
Corp user
Corporate BYOD user
Destination
AAA server DMZ segment
11
DMZ Switch
GM-N
6
WLC
Access point
DMZ-Segment
2
→ BYOD Authentication Encrypted traffic→ IP SEC from Firewall-11 till Firewall 2
BYOD Authentication traffic
Domestic MPLS Cloud advertise both network trusted and Untrusted BYOD segment (Pre-auth)
4
GM-2
Internal Zone
DMZ Firewall
DMZ External Zone
DMZ Swicth
External Firewall
LAN Switch
1
GM-5
3
GetvPN
Key Server
Anchor
Controller
Internet segment
7
DMZ Firewall
External Firewall
Anchor
Controller
Internet
Cluster Deployment BYOD Encryption solution Design
WLC
Post Authentication Internet traffic direct exit
8
Source
BYOD User
Vlan details: Corp BYOD Users
Pre-Auth: Vlan 200→192.168.0.0/16
Post-Auth: Vlan 201→172.28.0.0/16
Internet IP Pool: Public IP range

Figure 2: Simulated lab for this research

Below are the index used during the simulation

Table 4: Index used in Fgure-2

Index	Components	Used for
3	Key Server (Getvpn)	For policy management of encryption
4,5,6	Group Member	Get vpn Group members for encryption
1	Firewall	Internal Firewall for Segregation of DMZ (cisco)
2	Firewall	External checkpoint firewall for BYOD Internet traffic exit
7	Firewall	Branch level : External checkpoint firewall for BYOD Internet traffic exit
8,9	BYOD user	BYOD user from remote Branch
10.	Anchor controller	Anchoring traffic of BYOD
11	AAA server	Cisco Identity Service Engine used

During this research Getvpn infrastructure was used using 2 remote branch and 1 data center central. Key server was placed in same network for security policy management. AAA server was placed in central site. Authentication server was used as Identity service Engine. External firewall was used during the test as Checkpoint firewall.

III. RESULT AND ANALYSIS

3.1 PROTECTING CORPORATE NETWORK FROM BYOD UNTRUSTED AUTHENTICATION TRAFFIC

In this research protection of the network has been explored using GetVPN. As shown in fig-2 BYOD authentication traffic traversing from branch network to Data center over corporate MPLS network where AAA server placed are encrypted and segregated. Below result shows the encryption.

Encryption acl received on Getvpn GM as below

Table 5.1: Enforced policy ACL on GM (Figure 1 GM)

GETvpn-GM #show crypto gdoi gm acl
Group Name: GETVPN
ACL Downloaded From KS 10.1.1.2:
access-list deny udp any any port = 848
access-**list** **d**eny udp any port = 848 any
access-list deny tcp any any port = 179
access-list deny tcp any port = 179 any
access-list permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

After implementation observed enforced encryption policy for BYOD traffic on GM

Table 5.2: enforced policy of getvpn on GM

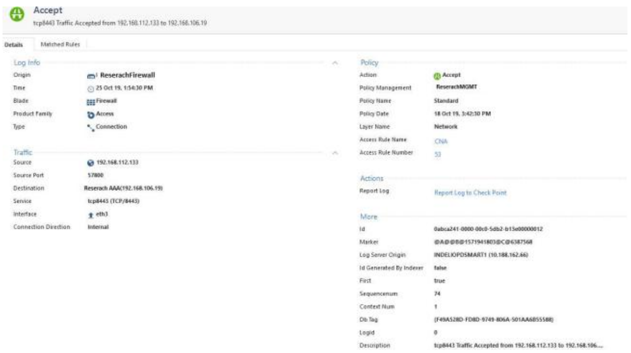
GETvpn-GM#show crypto ipsec sa
interface: GigabitEthernet0/0/0
Crypto map tag: Getvpn-Test, local addr 172.1.1.1
protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
Group: GETVPN
current_peer 0.0.0.0 port 848
PERMIT, flags={}
#pkts encaps: 735869984, #pkts encrypt: 735869984, #pkts digest: 735869984
#pkts decaps: 617390458, #pkts decrypt: 617390458, #pkts verify: 617390458
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 172.1.1.1, remote crypto endpt.: 0.0.0.0
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0
current outbound spi: **0x80B694D2**(2159449298)
PFS (Y/N): N, DH group: none
inbound esp sas:
spi: 0x80B694D2(2159449298)
transform: esp-aes esp-sha-hmac ,

DOI:10.35940/ijrte.D8151.118419

in use settings ={Tunnel, }
FFFFFFFF80000048, crypto map: Test-GETVPN
sa timing: remaining key lifetime (sec): 1709
Kilobyte Volume Rekey has been disabled
IV size: 16 bytes
replay detection support: N
Status: ACTIVE(ACTIVE)

After traversing the network authentication traffic has reached corporate data center firewall where central authentication server is placed.

Below record was captured during the research where authentication traffic on port 8443 reflects during on boarding of BYOD users



Accept

tcp8443 Traffic Accepted from 192.168.112.133 to 192.168.106.19

Details | Matched Rules

Log Info

Origin	ResearachFirewall
Time	25 Oct 19, 1:54:30 PM
Blade	Firewall
Product Family	Access
Type	Connection

Traffic

Source	192.168.112.133
Source Port	57800
Destination	Reserach AAA(192.168.106.19)
Service	tcp8443 (TCP/8443)
Interface	eth3
Connection Direction	Internal

Policy

Action	Accept
Policy Management	ReserachMGMT
Policy Name	Standard
Policy Date	18 Oct 19, 3:42:30 PM
Layer Name	Network
Access Rule Name	CNA
Access Rule Number	53

Actions

Report Log	Report Log to Check Point

More

Id	0abca241-0000-00c0-5db2-b15e00000012
Marker	@A@@B@1571941803@C@6387568
Log Server Origin	INDELIOPDSMART1 (10.188.162.66)
Id Generated By Indexer	false
First	true
Sequencenum	74
Context Num	1
Db Tag	{F49A528D-FD8D-9749-806A-501AA6B55588}
Logid	0
Description	tcp8443 Traffic Accepted from 192.168.112.133 to 192.168.106...

Figure 3: Pre-auth traffic logs towards AAA from Firewall logs (Fig-2, index 2-Firewall)

Table 6: BYOD onborading Traffic logs from Firewall (Figure 2, Index 2 Firewall)

Id:	0abca241-0100-00c0-5db2-92bf0037002c
Marker:	@A@@B@1571941803@C@3224900
Log Server Origin:	10.5.5.5
Time:	2019-10-25T06:14:23Z
Interface Direction:	outbound
Interface Name:	eth3
Connection Direction:	Internal
Id Generated By Indexer:false	
First:	true
Sequencenum:	110
Service ID:	tcp8443
Source:	192.168.112.129
Source Port:	33541
Destination:	192.168.106.19
Destination Port:	8443
IP Protocol:	6
Context Num:	1
Action:	Accept
Type:	Connection
Policy Name:	Standard
Policy Management:	ResearchMGMT
Db Tag:	{F49A528D-FD8D-9749-806A-501AA6B55588}
Policy Date:	2019-10-18T10:12:30Z
Blade:	Firewall
Origin:	ResearchFirewall
Service:	TCP/8443
Product Family:	Access
Logid:	0
Access Rule Name:	CNA
Access Rule Number:	53
Policy Rule UID:	18547ecc-3565-41ed-b234-97381e3c9a52
Layer Name:	Network
Interface:	eth3
Description:	tcp8443 Traffic Accepted from 192.168.112.129 to 192.168.106.19

3.2 DETECT AND CONTROL CRIRITAL ATTACK IN BYOD AND FORENSIC ANALYSIS

In this research we have done in-depth analysis of BYOD security infrastructure. During the traffic analysis of critical attack in nature was detected using wireshark. In this phase we captured 2 different critical categories of traffic as (a) Attack from External source to BYOD infrastructure (Internal) and again (b) attack traffic from Internal to External

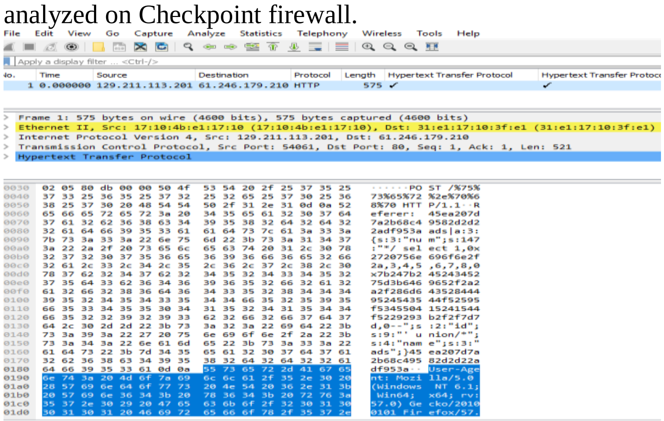
Traffic captured as below

Table 7: Traffic snip details

Sl No	Source	Destination	Attack type
1.	External	BYOD Infrastructure	Critical
2.	Internal BYOD	External network	Critical

3.2.A ATTACK FROM EXTERNAL TO INTERNAL

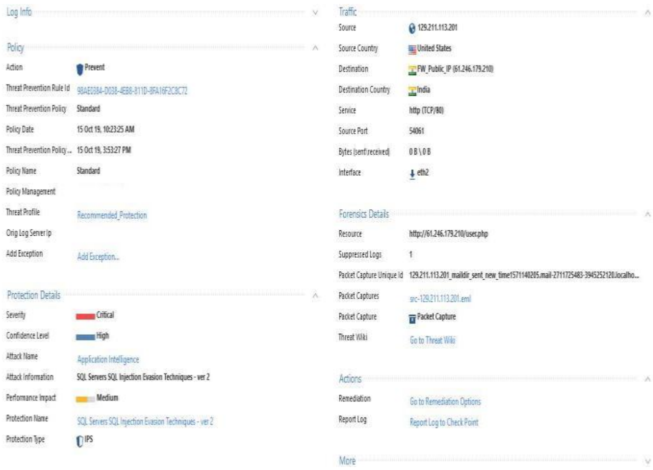
Here traffic is captured on Internal router shown in fig-3 (index 11). we snipped the traffic logs from router LAN side interface to detect traffic. Critical attack category traffic has been detected. Malicious activity was captured using wireshark[18] logs and analyzed.Multiple packets are captured and filtered out a particular packet from wireshark. Traffic source from 129.211.113.201 which is an attack source Ip in this case and the destination is 61.246.179.210. This packet is captured and the same is detected on figure 2 (index 2-external interface). The packet is http port 80 traffic. Packet captured are shown in below figure 4. Http header is checked of this packet and later same packet is analyzed on Checkpoint firewall.



```
No.   Time      Source          Destination     Protocol  Length  Hypertext Transfer Protocol  Hypertext Transfer Protoco
    1 0.000000  129.211.113.201 61.246.179.210  HTTP         575  ✓                            ✓

> Frame 1: 575 bytes on wire (4600 bits), 575 bytes captured (4600 bits)
> Ethernet II, Src: 17:10:4b:e1:17:10 (17:10:4b:e1:17:10), Dst: 31:e1:17:10:3f:e1 (31:e1:17:10:3f:e1)
> Internet Protocol Version 4, Src: 129.211.113.201, Dst: 61.246.179.210
> Transmission Control Protocol, Src Port: 54061, Dst Port: 80, Seq: 1, Ack: 1, Len: 521
> Hypertext Transfer Protocol

0030  02 05 80 db 00 00 50 4f  53 54 20 2f 25 37 35 25   ······PO ST /%75%
0040  37 33 25 36 35 25 37 32  25 32 65 25 37 30 25 36   73%65%72 %2e%70%6
0050  38 25 37 30 20 48 54 54  50 2f 31 2e 31 0d 0a 52   8%70 HTT P/1.1··R
0060  65 66 65 72 65 72 3a 20  34 35 65 61 32 30 37 64   eferer:  45ea207d
0070  37 61 32 62 36 38 63 34  39 35 38 32 64 32 64 32   7a2b68c4 9582d2d2
0080  32 61 64 66 39 35 33 61  61 64 73 7c 61 3a 33 3a   2adf953a ads|a:3:
0090  7b 73 3a 33 3a 22 6e 75  6d 22 3b 73 3a 31 34 37   {s:3:"nu m";s:147
00a0  3a 22 2a 2f 20 73 65 6c  65 63 74 20 31 2c 30 78   :"*/ sel ect 1,0x
00b0  32 37 32 30 37 35 36 65  36 39 36 66 36 65 32 66   2720756e 696f6e2f
00c0  32 61 2c 33 2c 34 2c 35  2c 36 2c 37 2c 38 2c 30   2a,3,4,5 ,6,7,8,0
00d0  78 37 62 32 34 37 62 32  34 35 32 34 33 34 35 32   x7b247b2 45243452
00e0  37 35 64 33 62 36 34 36  39 36 35 32 66 32 61 32   75d3b646 9652f2a2
00f0  61 32 66 32 38 36 64 36  34 33 35 32 38 34 34 34   a2f286d6 43528444
0100  39 35 32 34 35 34 33 35  34 34 66 35 32 35 39 35   95245435 44f52595
0110  66 35 33 34 35 35 30 34  31 35 32 34 31 35 34 34   f5345504 15241544
0120  66 35 32 32 39 32 39 33  62 32 66 32 66 37 64 37   f5229293 b2f2f7d7
0130  64 2c 30 2d 2d 22 3b 73  3a 32 3a 22 69 64 22 3b   d,0--";s :2:"id";
0140  73 3a 39 3a 22 27 20 75  6e 69 6f 6e 2f 2a 22 3b   s:9:"' u nion/*";
0150  73 3a 34 3a 22 6e 61 6d  65 22 3b 73 3a 33 3a 22   s:4:"nam e";s:3:"
0160  61 64 73 22 3b 7d 34 35  65 61 32 30 37 64 37 61   ads";}45 ea207d7a
0170  32 62 36 38 63 34 39 35  38 32 64 32 64 32 32 61   2b68c495 82d2d22a
0180  64 66 39 35 33 61 0d 0a  55 73 65 72 2d 41 67 65   df953a·· User-Age
0190  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0 
01a0  28 57 69 6e 64 6f 77 73  20 4e 54 20 36 2e 31 3b   (Windows  NT 6.1;
01b0  20 57 69 6e 36 34 3b 20  78 36 34 3b 20 72 76 3a    Win64;  x64; rv:
01c0  35 37 2e 30 29 20 47 65  63 6b 6f 2f 32 30 31 30   57.0) Ge cko/2010
01d0  30 31 30 31 20 46 69 72  65 66 6f 78 2f 35 37 2e   0101 Fir efox/57.
```

Figure 4: Packet captured using wireshark.(Interface of Fig2,Index 2)

The same packet when we checked on IPS blade of checkpoint firewall of the architecture shown in figure 2(index 2). We have found the malicious traffic which critical attack in nature.



Log Info

Policy
Action Prevent
Threat Prevention Rule Id 98AE0384-D038-4EB8-811D-8FA16F2C8C72
Threat Prevention Policy Standard
Policy Date 15 Oct 19, 10:23:25 AM
Threat Prevention Policy... 15 Oct 19, 3:53:27 PM
Policy Name Standard
Policy Management
Threat Profile Recommended_Protection
Orig Log Server Ip
Add Exception Add Exception...

Protection Details
Severity Critical
Confidence Level High
Attack Name Application Intelligence
Attack Information SQL Servers SQL Injection Evasion Techniques - ver 2
Performance Impact Medium
Protection Name SQL Servers SQL Injection Evasion Techniques - ver 2
Protection Type IPS

Traffic
Source 129.211.113.201
Source Country United States
Destination FW_Public_IP (61.246.179.210)
Destination Country India
Service http (TCP/80)
Source Port 54061
Bytes (sent\received) 0 B \ 0 B
Interface eth2

Forensics Details
Resource http://61.246.179.210/user.php
Suppressed Logs 1
Packet Capture Unique Id 129.211.113.201_maildir_sent_new_time1571140205.mail-2711725483-3945252120.localho...
Packet Captures src-129.211.113.201.eml
Packet Capture Packet Capture
Threat Wiki Go to Threat Wiki

Actions
Remediation Go to Remediation Options
Report Log Report Log to Check Point

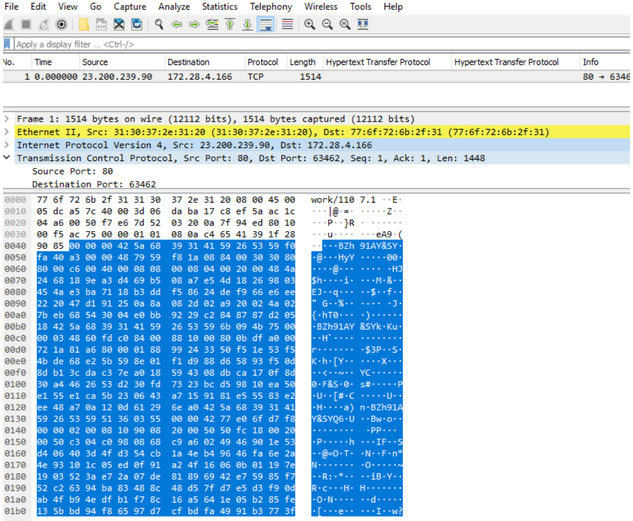
More

Figure 5: packet captured on checkpoint firewall (Fig2,Index2)

The category of attack is SQL Servers SQL Injection Evasion Techniques - ver 2[19] which was targeted to use commands on SQL servers by remote attackers by getting access. Forensic module details are also captured on checkpoint firewall which has detected the resource details targeted to access. Later this particular attack is blocked and evidence for this malicious activity was preserved on smart management server for further investigation as well without breaking chain of custody

3.2.B ATTACK FROM INTERNAL TO EXTERNAL

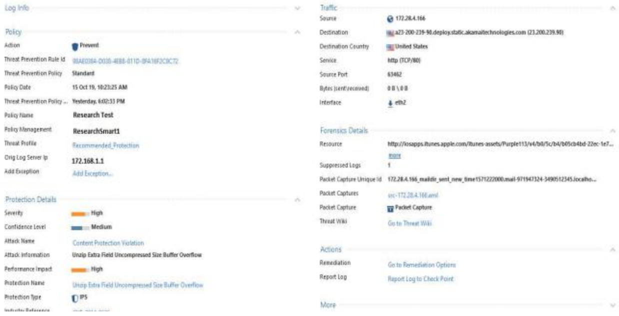
As most of the time trusted users insiders are more vulnerable and 62% attack are from insiders[4]. So in this research internal traffic threat was analyzed to investigate and find evidence of the malicious activity. Same type of packet captured was conducted to find malicious traffic . This time packet was capture on internal interface of the firewall(Figure 2, 2) and filtered out a packet and analyzed in wireshark logs as shown belowThis time return traffic was captured and investigated


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time     Source          Destination   Protocol  Length  Hypertext Transfer Protocol  Hypertext Transfer Protocol  Info
   1 0.000000 23.200.239.90   172.28.4.166  TCP       1514                                                              80 → 6346

> Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: 31:30:37:2e:31:20 (31:30:37:2e:31:20), Dst: 77:6f:72:6b:2f:31 (77:6f:72:6b:2f:31)
> Internet Protocol Version 4, Src: 23.200.239.90, Dst: 172.28.4.166
v Transmission Control Protocol, Src Port: 80, Dst Port: 63462, Seq: 1, Ack: 1, Len: 1448
    Source Port: 80
    Destination Port: 63462

0000  77 6f 72 6b 2f 31 31 30  37 2e 31 20 08 00 45 00   work/110 7.1 ··E·
0010  05 dc a5 7c 40 00 3d 06  da ba 17 c8 ef 5a ac 1c   ···|@·=· ·····Z··
0020  04 a6 00 50 f7 e6 7d 52  03 20 0a 7f 94 ed 80 10   ···P··}R · ······
0030  00 f5 ac 75 00 00 01 01  08 0a c4 65 41 39 1f 28   ···u···· ···eA9·(
0040  90 85 00 00 00 42 5a 68  39 31 41 59 26 53 59 f0   ·····BZh 91AY&SY·
0050  fa 40 a3 00 00 48 79 59  f8 1a 08 84 00 30 30 80   ·@···HyY ·····00·
0060  80 00 c6 00 40 00 08 08  00 08 04 00 20 00 48 4a   ····@··· ···· ·HJ
0070  24 68 18 9e a3 d4 69 b5  08 a7 e5 4d 18 26 98 03   $h····i· ···M·&··
0080  45 4a e3 ba 71 18 b3 dd  f5 86 24 de f9 66 e6 ee   EJ··q··· ··$··f··
0090  22 20 47 d1 91 25 0a 8a  08 2d 02 a9 20 02 4a 02   " G··%·· ·-·· ·J·
00a0  7b eb 68 54 30 04 e0 bb  92 29 c2 84 87 87 d2 05   {·hT0··· ·)······
00b0  18 42 5a 68 39 31 41 59  26 53 59 6b 09 4b 75 00   ·BZh91AY &SYk·Ku·
00c0  00 03 48 60 fd c0 84 00  88 10 00 80 0b df a0 00   ··H`···· ········
00d0  72 1a 81 a6 80 00 01 88  99 24 33 50 f5 1e 53 f5   r······· ·$3P··S·
00e0  4b de 68 e2 5b 59 8e 01  f1 d9 88 d6 58 93 f5 0d   K·h·[Y·· ····X···
00f0  8d b1 3c da c3 7e a0 18  59 43 08 db ca 17 0f 8d   ··<··~·· YC······
0100  30 a4 46 26 53 d2 30 fd  73 23 bc d5 98 10 ea 50   0·F&S·0· s#·····P
0110  e1 55 e1 ca 5b 23 06 43  a7 15 91 81 e5 55 83 e2   ·U··[#·C ·····U··
0120  ee 48 a7 0a 12 0d 61 29  6e a0 42 5a 68 39 31 41   ·H····a) n·BZh91A
0130  59 26 53 59 51 36 03 55  00 00 42 77 e0 6f d7 f8   Y&SYQ6·U ··Bw·o··
0140  00 00 02 00 08 10 90 08  20 00 50 50 fc 18 00 20   ········  ·PP···
0150  00 50 c3 04 c0 98 08 68  c9 a6 02 49 46 90 1e 53   ·P·····h ···IF··S
0160  d4 06 40 3d 4f d3 54 cb  1a 4e b4 96 46 fa 6e 2a   ··@=O·T· ·N··F·n*
0170  4e 93 10 1c 05 ed 0f 91  a2 4f 16 06 0b 01 19 7e   N······· ·O·····~
0180  19 03 52 3a e7 2a 07 de  81 89 69 42 e7 59 85 f7   ··R:·*·· ··iB·Y··
0190  52 c2 63 94 ba 83 48 8c  48 d5 7f d7 e5 d3 f9 0d   R·c···H· H·······
01a0  ab 4f b9 4e df b1 f7 8c  16 a5 64 1e 05 b2 85 fe   ·O·N···· ··d·····
01b0  13 5b bd 94 f8 65 97 d7  cf bd fa 49 91 b3 77 3f   ·[···e·· ···I··w?
```

Figure 6 : Malicious activity internal to external (Return traffic).

The same packet forensic analysis was captured on Checkpoint firewall (Fig 2,2) and shown as below



Log Info

Policy
Action Prevent
Threat Prevention Rule Id 98AE0384-D038-4EB8-811D-8FA16F2C8C72
Threat Prevention Policy Standard
Policy Date 15 Oct 19, 10:23:25 AM
Threat Prevention Policy ... Yesterday, 6:02:33 PM
Policy Name Research Test
Policy Management ResearchSmart1
Threat Profile Recommended_Protection
Orig Log Server Ip 172.168.1.1
Add Exception Add Exception...

Protection Details
Severity High
Confidence Level Medium
Attack Name Content Protection Violation
Attack Information Unzip Extra Field Uncompressed Size Buffer Overflow
Performance Impact High
Protection Name Unzip Extra Field Uncompressed Size Buffer Overflow
Protection Type IPS

Traffic
Source 172.28.4.166
Destination a23-200-239-90.deploy.static.akamaitechnologies.com (23.200.239.90)
Destination Country United States
Service http (TCP/80)
Source Port 63462
Bytes (sent\received) 0 B \ 0 B
Interface eth2

Forensics Details
Resource http://iosapps.itunes.apple.com/itunes-assets/Purple113/v4/b0/5c/b4/b05cb4bd-22ec-1e7... more
Suppressed Logs 1
Packet Capture Unique Id 172.28.4.166_maildir_sent_new_time1571222000.mail-971947324-3490512345.localho...
Packet Captures src-172.28.4.166.eml
Packet Capture Packet Capture
Threat Wiki Go to Threat Wiki

Actions
Remediation Go to Remediation Options
Report Log Report Log to Check Point

More

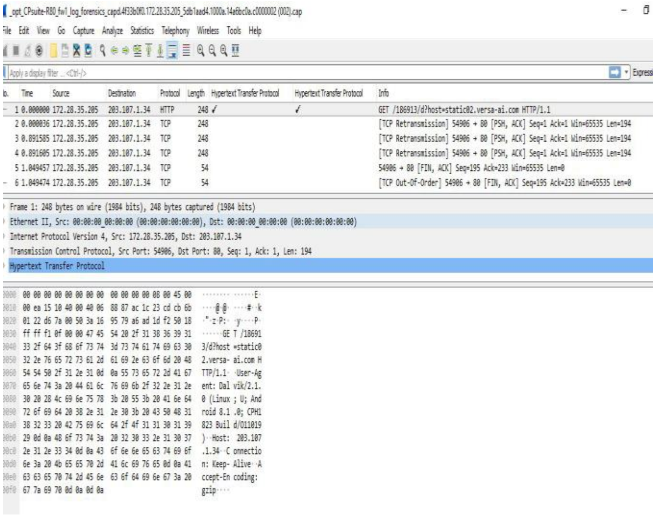
Figure 7: 1st packet of BYOD malicious traffic from internal to external.

In this analysis internal BYOD user who got IP address of 172.28.4.166 and destination IP 23.200.239.90 and attack was content protection violation which was critical in nature. This malicious activity was performed by BYOD user as buffer overflow vulnerability[20]. This was an acknowledgement packet and forensic information was analysed. Importance of keeping the evidence for further analysis was an important requirement and same was available for further analysis and protection as well.

BYOD post authentication users were intended to be trusted but these users were performing malicious activity which was risk for the organization.

3.2.C APPLICATION LAYER MALICIOUS ACTIVITY FORENSIC

Application layer threat was analyzed and captured on ingress interface of the firewall shown in fig 3 (index 8) and below was the result traffic sourcing from one of the BYOD user having IP address of 172.28.35.205 to the destination 203.107.1.34.

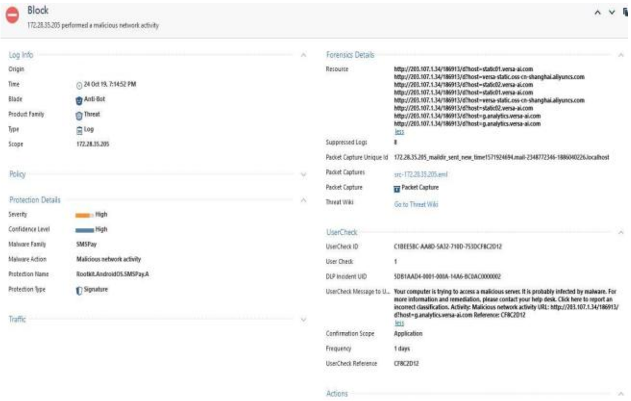

_opt_CPsuite-R80_fw1_log_forensics_capd.4f33b0f0.172.28.35.205_5db1aad4.1000a.14a6bc0a.c0000002 (002).cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expressi

```
No. Time     Source         Destination   Protocol Length Hypertext Transfer Protocol Hypertext Transfer Protocol Info
  1 0.000000 172.28.35.205  203.107.1.34  HTTP     248    ✓                           ✓                           GET /186913/d?host=static02.versa-ai.com HTTP/1.1
  2 0.000036 172.28.35.205  203.107.1.34  TCP      248                                                            [TCP Retransmission] 54906 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=194
  3 0.891585 172.28.35.205  203.107.1.34  TCP      248                                                            [TCP Retransmission] 54906 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=194
  4 0.891605 172.28.35.205  203.107.1.34  TCP      248                                                            [TCP Retransmission] 54906 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=194
  5 1.049457 172.28.35.205  203.107.1.34  TCP       54                                                            54906 → 80 [FIN, ACK] Seq=195 Ack=233 Win=65535 Len=0
  6 1.049474 172.28.35.205  203.107.1.34  TCP       54                                                            [TCP Out-Of-Order] 54906 → 80 [FIN, ACK] Seq=195 Ack=233 Win=65535 Len=0

> Frame 1: 248 bytes on wire (1984 bits), 248 bytes captured (1984 bits)
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 172.28.35.205, Dst: 203.107.1.34
> Transmission Control Protocol, Src Port: 54906, Dst Port: 80, Seq: 1, Ack: 1, Len: 194
> Hypertext Transfer Protocol

0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ········ ······E·
0010  00 ea 15 10 40 00 40 06  88 87 ac 1c 23 cd cb 6b   ····@·@· ····#··k
0020  01 22 d6 7a 00 50 3a 16  95 79 a6 ad 1d f2 50 18   ·"·z·P:· ·y····P·
0030  ff ff f1 0f 00 00 47 45  54 20 2f 31 38 36 39 31   ······GE T /18691
0040  33 2f 64 3f 68 6f 73 74  3d 73 74 61 74 69 63 30   3/d?host =static0
0050  32 2e 76 65 72 73 61 2d  61 69 2e 63 6f 6d 20 48   2.versa- ai.com H
0060  54 54 50 2f 31 2e 31 0d  0a 55 73 65 72 2d 41 67   TTP/1.1· ·User-Ag
0070  65 6e 74 3a 20 44 61 6c  76 69 6b 2f 32 2e 31 2e   ent: Dal vik/2.1.
0080  30 20 28 4c 69 6e 75 78  3b 20 55 3b 20 41 6e 64   0 (Linux ; U; And
0090  72 6f 69 64 20 38 2e 31  2e 30 3b 20 43 50 48 31   roid 8.1 .0; CPH1
00a0  38 32 33 20 42 75 69 6c  64 2f 4f 31 31 30 31 39   823 Buil d/O11019
00b0  29 0d 0a 48 6f 73 74 3a  20 32 30 33 2e 31 30 37   )··Host:  203.107
00c0  2e 31 2e 33 34 0d 0a 43  6f 6e 6e 65 63 74 69 6f   .1.34··C onnectio
00d0  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d 0a 41   n: Keep- Alive··A
00e0  63 63 65 70 74 2d 45 6e  63 6f 64 69 6e 67 3a 20   ccept-En coding:
00f0  67 7a 69 70 0d 0a 0d 0a                            gzip····
```

Figure 8: attack captured on ingress interface of Checkpoint firewall

Same packet was analyzed on the checkpoint firewall and found this was a serious malware category malicious activity.The forensic threat emulation was enabled on checkpoint firewall to detect the malicious activity and forensic logs was seen on this blade. Below result was found which again blocked using application control blade.

As seen traffic sourcing from 172.28.35.205 destined to 203.107.1.34.



Block
172.28.35.205 performed a malicious network activity

Log Info
Origin
Time: 24 Oct 19, 7:14:52 PM
Blade: Anti-Bot
Product Family: Threat
Type: Log
Scope: 172.28.35.205

Policy

Protection Details
Severity: High
Confidence Level: High
Malware Family: SMSPay
Malware Action: Malicious network activity
Protection Name: Rootkit.AndroidOS.SMSPay.A
Protection Type: Signature

Traffic

Forensics Details
Resource:
http://203.107.1.34/186913/d?host=static01.versa-ai.com
http://203.107.1.34/186913/d?host=versa-static.oss-cn-shanghai.aliyuncs.com
http://203.107.1.34/186913/d?host=static02.versa-ai.com
http://203.107.1.34/186913/d?host=static01.versa-ai.com
http://203.107.1.34/186913/d?host=versa-static.oss-cn-shanghai.aliyuncs.com
http://203.107.1.34/186913/d?host=static02.versa-ai.com
http://203.107.1.34/186913/d?host=g.analytics.versa-ai.com
http://203.107.1.34/186913/d?host=g.analytics.versa-ai.com
less
Suppressed Logs: 8
Packet Capture Unique Id: 172.28.35.205_maildir_sent_new_time1571924694.mail-2348772346-1886040226.localhost
Packet Captures: src-172.28.35.205.eml
Packet Capture: Packet Capture
Threat Wiki: Go to Threat Wiki

UserCheck
UserCheck ID: C1BEE5BC-AA8D-5A32-710D-753DCF8C2D12
User Check: 1
DLP Incident UID: 5DB1AAD4-0001-000A-14A6-BC0AC0000002
UserCheck Message to U...: Your computer is trying to access a malicious server. It is probably infected by malware. For more information and remediation, please contact your help desk. Click here to report an incorrect classification. Activity: Malicious network activity URL: http://203.107.1.34/186913/d?host=g.analytics.versa-ai.com Reference: CF8C2D12
less
Confirmation Scope: Application
Frequency: 1 days
UserCheck Reference: CF8C2D12

Actions

Figure 9: Detection and blocked the attack on Checkpoint external firewall(Fig 2, 2).

IV. DISCUSSION

First objective of this study was to minimize the security risk in Cluster deployment of BYOD infrastructure using encryption method.In this study we have explored encryption mechanism adoption for BYOD traffic. While BYOD is deployed in cluster where authentication server is central and authentication traffic is coming from remote branch to central data center, BYOD traffic is traversing with corporate network. Organization MPLS network carrying traffic for both the network where risk is more.

Second objective of this research was detection of malicious activity, then protect and explored the Forensic investigation of BYOD malicious traffic.

Detection of Cyber attack in the BYOD environment is most critical task, Study on BYOD security risk in Airport Security which is a major risk of the country[21] due to BYOD. Also another study says BYOD might become "Bring your own danger"[22] if control security is not implemented and if not prepared for forensic investigation after an attack, so this study has a significant result of detecting malicious activity using application layer of detection mechanism.

4.1 CONTRIBUTION

Contribution of this research in BYOD infrastructure is securing corporate network from BYOD untrusted authentication traffic using reverse adoption of encryption mechanism for BYOD traffic not corporate MPLS. This method segregate traffic between corporate network and BYOD network from Branch to Data center. As a result security risk gets reduced.2nd contribution of this research is to detect and protect malicious activities in BYOD infrastructure and forensic investigation using threat emulation.

4.2 FUTURE RESEARCH

Future research in this direction is to explore advance forensic investigation model inline with corporate Cyber Law. Detection of cyber attack in BYOD infrastructure forensic investigation model is on demand in the study, which can be further explored in details.

V. CONCLUSION

A secured authentication model is required to protect corporate network infrastructure and reduce cyber risk due to adoption of BYOD. In this paper we have presented a model of reverse adoption of encryption technique of BYOD traffic while traversing through corporate MPLS network. Segregated the corporate network from BYOD traffic using a reverse adoption of encryption mechanism. This makes the BYOD authentication traffic securely reaching the central AAA server without touching corporate network. Security risk is reduced using this encryption method and corporate network becomes risk free and provide Cyber secured BYOD environment.

Second part of the research has explored the detection of malicious activities and protect the BYOD infrastructure. 2nd part of the research has contributed to build digital forensic readiness BYOD infrastructure to conduct investigation post attack.

ACKNOWLEDGEMENT

The research, hypothesis, assessments and analysis articulated in this paper are those of the authors alone and not the organization with whom the authors are associated.

REFERENCES

1. H. Shetty, L. Unden-Farboud, and P. Arriandiaga, "Competitive Landscape: Managed Mobility Services," p. 20.
2. "94% enterprises will use IoT by end 2021: Microsoft report," https://www.livemint.com. [Online]. Available: https://www.livemint.com/technology/tech-news/94-enterprises-will-use-iot-by-end-2021-microsoft-report-1565165449842.html. [Accessed: 08-Aug-2019].
3. B. Tokuyoshi, "The security implications of BYOD," Network Security, vol. 2013, no. 4, pp. 12–13, Apr. 2013.
4. J. Collie, "A Strategic Model for Forensic Readiness," Athens Journal of Sciences, vol. 5, no. 2, pp. 167–182, Jun. 2018.
5. U. Raj, "Certificate based hybrid authentication for Bring Your Own Device (BYOD) in Wi-Fi enabled Environment," vol. 13, no. 12, p. 7, 2015.
6. "BYOD Secured Solution Framework," International Journal of Engineering and Advanced Technology, vol. 8, no. 6, pp. 1602–1606, Aug. 2019.
7. "International Journal of Scientific Research in Computer Science, Engineering and Information Technology," p. 7, 2018.
8. K. AlHarthy and W. Shawkat, "Implement network security control solutions in BYOD environment," in 2013 IEEE International Conference on Control System, Computing and Engineering, Penang, Malaysia, 2013, pp. 7–11.
9. P. K. Gajar, A. Ghosh, and S. Rai, "BRING YOUR OWN DEVICE (BYOD): SECURITY RISKS AND MITIGATING STRATEGIES," p. 9, 2010.
10. K. Joshi, M. Pathak, S. Jose, S. Dahiya, and S. Jose, "(71) Applicant: Gigamon Inc., Santa Clara, CA (US)," p. 18.
11. M. Mahinderjit Singh, S. Sin Siang, O. Ying San, N. H. A. Hassain Malim, and A. R. Mohd Shariff, "Security Attacks Taxonomy on Bring Your Own Devices (BYOD) Model," International Journal of Mobile Network Communications & Telematics, vol. 4, no. 5, pp. 1–17, Oct. 2014.
12. F. Jamal, M. T. Abdullah, A. Abdullah, and Z. M. Hanapi, "BYOD Authentication Process (BAP) Using Blockchain Technology," Control Systems, vol. 10, no. 11, p. 8, 2018.
13. F. Jamal, M. T. Abdullah, A. Abdullah, and Z. M. Hanapi, "Enhanced Bring your Own Device (BYOD) Environment Security based on Blockchain Technology," International Journal of Engineering, p. 6.
14. M. Ratchford, P. Wang, and R. O. Sbeit, "BYOD Security Risks and Mitigations," in Information Technology - New Generations, vol. 558, S. Latifi, Ed. Cham: Springer International Publishing, 2018, pp. 193–197.
15. M. P. Souppaya and K. A. Scarfone, "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security," National Institute of Standards and Technology, NIST SP 800-46r2, Jul. 2016.

16. “Group Encrypted Transport VPN (Get VPN) Design and Implementation Guide,” p. 165.
17. “Cisco SAFE Reference Guide,” p. 354.
18. “Wireshark · Go Deep.” [Online]. Available: https://www.wireshark.org/. [Accessed: 06-Oct-2019].
19. “Search: SQL Servers SQL Injection Evasion Techniques - ver 2 | Check Point ThreatPoint.” [Online]. Available: https://threatpoint.checkpoint.com/ThreatPortal/search?pattern=SQL%20Servers%20SQL%20Injection%20Evasion%20Techniques%20-%20ver%202&type=all&page=0&utm_source=cp_logs. [Accessed: 19-Oct-2019].
20. “Search: Unzip Extra Field Uncompressed Size Buffer Overflow | Check Point ThreatPoint.” [Online]. Available: https://threatpoint.checkpoint.com/ThreatPortal/search?pattern=Unzip%20Extra%20Field%20Uncompressed%20Size%20Buffer%20Overflow&type=all&page=0&utm_source=cp_logs. [Accessed: 19-Oct-2019].
21. G. Suciu, A. Scheianu, I. Petre, L. Chiva, and C. S. Bosoc, “Cybersecurity Threats Analysis for Airports,” in New Knowledge in Information Systems and Technologies, vol. 931, Á. Rocha, H. Adeli, L. P. Reis, and S. Costanzo, Eds. Cham: Springer International Publishing, 2019, pp. 252–262.
22. P. Beckett, “BYOD – popular and problematic,” Network Security, vol. 2014, no. 9, pp. 7–9, Sep. 2014.

AUTHORS PROFILE

Md Iman Ali is a Research scholar, in the department of computer application at Lovely Professional University, Punjab, India. He has completed MCA and DOEACC “A” level. As a professional certification he is CCIE Lab certified. He is working as an Associate Director, Technology, KPMG India. His research interest area include BYOD secured solutions, Digital Forensic, Cyber Forensic, Cyber security, SD-WAN Security, Cloud Security and Smart city Cyber Forensic.

Dr. Sukhkirandeep Kaur, is an assistant professor in Department of Computer Science and Engineering, Lovely Professional University, Phagwara. She received her PhD from National Institute of Technology, Srinagar. She has authored over 10 papers in international journals and conferences. Her research interest includes Wireless Sensor Networks, Internet of Things and Artificial Intelligence, Cyber Security, Cyber Forensic, BYOD.