Security Challenges and Cyber Forensic Ecosystem in IoT Driven BYOD Environment

MD IMAN ALI1, SUKHIRANDEEP KAUR2, ADITYA KHAMPARIA2, DEEPAK GUPTA3, (Member, IEEE), SACHIN KUMAR4, ASHISH KHANNA3, (Member, IEEE), AND FADI AL-TURJMAN5, (Member, IEEE)

1Department of Computer Application, Lovely Professional University, Phagwara 144001, India
2School of Computer Science and Engineering, Lovely Professional University, Phagwara 144001, India
3Maharastra Agrasen Institute of Technology, New Delhi 110086, India
4Department of Computer Science, South Ural State University, 454080 Chelyabinsk, Russia
5Artificial Intelligence Department, Research Center for AI and IoT, Near East University, 99138 Nicosia, Turkey

Corresponding authors: Aditya Khamparia (aditya.khamparia88@gmail.com) and Sachin Kumar (sachinagnihotri16@gmail.com)

This work was supported in part by the Ministry of Science and Higher Education of the Russian Federation (government order FENU-2020-0022).

ABSTRACT The usage of Internet of Things (IoT)/ Bring Your Own Devices (BYOD) has grown up exponentially, as expected 50 Billion IoT devices will get connected by the end of 2020 in the world in smart city environment. Advancement of Human Driven Edge Computing (HEC) with 5th Generation Internet services also makes this more feasible. Use of IoT and increased demand of BYOD becomes one of the fundamental needs to increase the organization employee productivity and business agility. But it increased the significant risk of the cyber-attack which is leading a major reason for business disruption and becomes a leading question about how to get a cyber secured citizenship in the smart city environment as well as in the organization where BYOD is used in large numbers. In order to conduct forensic investigation post incident detection of malicious activities from IoT/BYOD end point is most challenging task. A strategic practical approach in this research is presented to detect malicious activities so that organization can adopt to protect the critical infrastructure and smart city critical infrastructure. In order to achieve the goal of detecting of malicious activities in BYOD environment, simulation performed in 3 phases. The 1st phase of the simulation performed while BYOD endpoint was outside the organization over the internet without VPN. The 2nd phase of the simulation was performed where BYOD endpoint was securely onboarded using a corporate wireless network with a secured onboarding process. The 3rd phase of the test done where IoT/BYOD was outside the organization with a VPN. A unique robust scalable model puts forward with significant result from this research and concluded for creating a cyber forensic ecosystem in IoT/BYOD environment to enable cyber secured citizenship in era of HEC with 5G and IoT.

INDEX TERMS Security challenges, IoT, digital forensic, encryption, BYOD.

I. INTRODUCTION

The world hits 3rd Major global risk [1] as defined in the Global Risk Report of World Economic Forum’2019 due to COVID-19 pandemic outbreaks on 11th March’20 by World Health Organization [2]. The entire world is in locked downstage while various government has declared locked down in regional country [3] to break the chain of Covid-19 to reduce the impact of pandemic damage. This pandemic has changed the complete business ecosystem and the enterprise working model turned into an alternate method of working from the home environment using BYOD. But this alternate method of working environment with larger population has created a major cyber security which is also one of the major business disruption reason stated in Global risk landscape [1].

Top 3rd major global risk [4] emerged due to Covid-19 WFH (Work from home) alternate method of the working environment and the cyber threat becomes business disruption reason.

Cyber-attacks are consistently becoming a global risk factor as per the study of Cyber threat global risk index. And the index of Cyber-attacks risk trigger to explore more into this area as shown in Fig. 1.

Consistently cyber attack always ranked as global risk and due to COVID-19 pandemic situation this becomes more
vulnerable and attackers were targeting organizations due to changing traffic patterns during WFH.

As the entire world is battling against Covid-19 global pandemic and lockdown has turned to enabled enterprise, government critical infrastructure to enable working from home using remote VPN services or to enable the option to use Bring Your own devices and enable corporate infrastructure access from BYOD.

Different VPN services have been enabled like cisco anyconnect on-premise solution and Global Protect Palo alto VPN services.

During covid-19 lockdown in the world cisco anyconnect usage has increased, cisco has also opened up the channel to support market [6]. Threat Roundup of cisco Tallos [7] again reported a new threat due to an increased amount of load and traffic patterns changed.

Due to the Covid-19 Lockdown alternate method of the working environment (WFH) option traffic pattern changed in the reverse direction, in some cases hybrid model of traffic has opened up a new threat corridor.

The recent cyber incident in cognizant technologies has revealed that cyber threat landscape has started adopting a new model of attack. Major security practice player organization like Cognizant [8] was hitting Maze Ransomware attack on 18th April'20 [9] during Covid-19.

The Covid-19 Pandemic situation has triggered to re-architect the traditional IT infrastructure to build a cyber-confidence techno-centric architecture to build an alternate method of the work environment so that the business ecosystem can be drive through remotely and enable the BYOD services widely.

The prediction was clear in 2018 by Gartner for the adoption of BYOD services by 2022 [10] are expected to grow from 35% to 75%. Due to multiple reasons, By 2021 [11] almost all the entities are expected to use IoT, as per Microsoft 94% of the organization will adopt IoT. BYOD devices are unmanaged devices which might have more vulnerabilities and may not have minimum security defense mechanism and have malicious content [12]. Once BYOD is on boarded this becomes corporate trusted devices and insiders are riskier as 62% of digital incidents are due to the inside users [13].

A. PREVIOUS STUDY

1) A BYOD CERTIFICATE BASED 3 TIER SECURED Model
The framework of the secured authentication model was explored and onboarding was done securely [14] of BYOD internal users. The multi-factor authentication model with a Certificate-based Hybrid model of authentication was one of the successful models with 3 tier captcha [15]. Apart from this secure communication mechanism with a dual-factor authentication method has been explored using Scyther Tool and the dual-factor authentication mechanism was tested for automatic verification tools with a secured approach in IoT [16] environment. While BYOD is in LAN secured model of onboarding was also explored using 802.1x authentication security control [17] mechanism.

2) SECURE BYOD WITH ENCRYPTION MODEL
Encryption of corporate data in BYOD was a successful model to secure corporate data [18]. End to end encryption and cryptographic method of network security is an option in recent research in 2019 also a secured model [19]. During remote access services Denial-of-Service Attack (DDoS) attack network traffic gets congested in remote site traffic authentication traversing was critical aspect [20] which was explored and mitigation with IDS/IPS.

3) BLOCKCHAIN BASED AUTHENTICATION FOR BYOD USERS
The block chain based Multi-factor authentication model was one of the successful models to authenticate BYOD with additional security [21] in the BYOD environment. The self-service portal based authentication model was another aspect studied to reduce the risk of data leakage and protect unauthorized access [22].

4) DECEPTION TECHNOLOGY
During 2016 detection of threat in BYOD infrastructure explored with deception technology called Honeypot technology. Analysis of root cause post detection was in important aspect in this study [23] integration of honeypot with cyber risk management process of FEMA mission where five preparedness (Federal emergency management agency) [24] was also studied subsequently. Extended next level research was also conducted in 2019 which was improved version in the study of “A Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology [23]”. Also in same direction Intelligent Threat Platform was another study for detecting the incident where accuracy has been analyzed [25]. To increases the accuracy level of malicious activities using audit logs collected from Intelligent Threat sources, accuracy has been analyzed as 90.73%, 96.16 and 93.71% [25].

5) THREAT INTERACTION MODEL
Threat interaction model proposed for analyzing different threats is very important study in Stride based model [26] in BYOD environment where internal and external threat
interaction was studied which further helped in forensics analysis. Adoption of GetVPN [27] in BYOD where segregation of traffic was another novel study. Encryption with Getvpn [27] in isolating of corporate traffic from untrusted traffic is a reverse adoption for diversification of external and internal traffic [28].

BYOD malicious activity detection mechanism different tools, method, technology already exist and developed which are available. But digital forensic ecosystem needs more advance level of detection mechanism, unfortunately due to current trend of threat advancement this is an impending area for building a reliable forensic ecosystem due to threat heterogeneous landscape, complexity and advancement. This required considerable dedicated consistent attention towards inclusion of new abstract so that digital forensic evidence with end to end back-trace capability can be developed with more accurate potential threat detection mechanism. Strongly suspected quite possible to stumble potential evidence related to forensic due to lack of correlation of logs from different components used in the BYOD infrastructure. What make investigation in difficult or some time failure that back trace of logs and identity. Also due to huge amount of data, logs, traffic logs from various components, lake of integration investigation becomes challenging.

In this paper, we present a practical approach of detecting malicious activities in the BYOD environment in order to develop and advancement of cyber forensic ecosystem so that challenging phase in forensic can be tackled seamlessly. We also aimed even in a situation like covid-19 lock-down phase where BYOD end points users need to onboard remotely, a systematic secured mechanism can be developed so that every malicious events are captured and diversified model can be opt by the organization to protect the critical infrastructure. Finally a model of BYOD forensic ecosystem is proposed to combat with current trend of threat landscape and corporate organization can be protected from potential damage due to cyber threat.

The paper is organized as follows: Introduction with Related works are in Section 1. Section 2 describe the Design and Implementation methods. In section 3 Result and analysis are presented. Section 4 deals with Discussion part. In section 5 Contribution of the research is described. In section 6 future research direction explained. And finally section 7 conclude the whole paper followed by acknowledgment section 8.

II. DESIGN AND IMPLEMENTATION METHODOLOGY
During the research, the simulation was conducted in 3 phases. BYOD infrastructure was built for detailed analysis of detecting the suspicious traffic. Different directions of traffic, the pattern of attack is the main concern for diversified testing. So that end of the simulation best possible result can be captured for analysis and cyber threat model can be industrialized.

A. PHASE 1: BYOD USERS OVER INTERNET WITHOUT VPN
In this phase, BYOD users were tested putting the users outside the organization using a personal device connected to the corporate network without VPN (Virtual Private Network) services.

B. PHASE 2: BYOD USERS OVER THE CORPORATE NETWORK
In this phase, BYOD users were placed inside the organization’s corporate wireless network using personal untrusted devices and malicious activities inspected.

C. PHASE 3: BYOD USERS OVER THE INTERNET WITH VPN
In this phase, BYOD users were placed over the internet with VPN services and connected to the corporate network and suspicious activities inspected.

D. PHASE 1: TEST
In the First phase, the method of research to onboard the BYOD users sitting in a remote area and using their personal devices and hook on corporate infrastructure using multi-layer security. Especially in the COVID-19 WFH option to enable this architecture was build and tested.

Due to COVID-19 organization looking for onboarding BYOD users from remotely while before COVID-19 these BYOD users were getting onboarded from the corporate network. But the difference was the BYOD users were getting on-boarded from remote area.

1) ARCHITECTURE OF THE BYOD FROM INTERNET WITHOUT VPN
The architecture was used during the research was as mentioned in Fig. 2.

![Figure 2. BYOD onboarding architecture.](image-url)
First Authentication process completed with an internal Active Directory of the remote users securely using Access connector placed in the DMZ segment of the corporate network. Once the Authentication process was successful then the actual traffic flow between BYOD users and the internal network was tested securely. In Second step during the test monitoring and detection of threats were conducted using cloud external security integration using GCP (Google Cloud Platform).

**a: BYOD AUTHENTICATION TRAFFIC ENCRYPTION TO REDUCE CYBER RISK**

Authentication was a critical process of onboarding and encryption mechanism was used during authentication [29] for the first level of risk mitigation [30].

Traffic flow used during this test mentioned in the below table.

| Index | Description                           |
|-------|---------------------------------------|
| 1.    | BYOD Remote Users                    |
| 2.    | Cloud onboarding workspace services  |
| 3.    | Authentication Request               |
| 4.    | DMZ segment Workspace Access connector |
| 5.    | Authentication to Active Directory    |
| 6.    | Internal Active Directory            |
| 7.    | Post Authentication traffic          |
| 8.    | Enterprise DMZ firewall              |
| 9.    | Internal Firewall                    |
| 10.   | Internal Application                 |
| 11.   | MPLS Cloud trusted                   |
| 12.   | Remote Branches                      |
| 13.   | Cloud based traffic                  |
| 14.   | SaaS based traffic                   |
| 15.   | Cloud Security                       |

**b: HOW END TO END BYOD SERVICES ENABLED**

BYOD users initially request for authentication to access the services, the cloud access enabler received the request. In 2nd part Access request forwards to organization DMZ access connector mentioned in Fig. 2 index 3. The Access connector sends the request back to back to the internal Active Directory as shown in Fig. 2 Index 4. Once the request is processed then authentication pass the message sent to the BYOD user. In 2nd session, BYOD users directly establish the connection to the internal corporate network to access the resources.

During the secure connection establishment a DMZ Access Secure gateway was used. DMZ secure gateway was establishing the connection between BYOD and internal network for secure connection.

**c: CLOUD SECURITY EMBEDDED TO SECURE THE INFRASTRUCTURE**

During the research cloud security model was an important viewpoint of securing the infrastructure of untrusted devices. The secured onboarding process was a critical component so the Cloud security model was embedded to enforce the security of untrusted devices to onboard.

While the traffic was hitting cloud workspace before sending this traffic to organization DMZ access connector used for identity check from Active directory. Traffic was routed through the cloud security Firewall as shown in Fig. 2 index 15. All minimum posture security check was conducted on this firewall.

During this test, the Palo Alto firewall was used for security control.

Parameter configured during the test is shown in the below figure.

**FIGURE 3.** HIP conditional parameter for security check. This important condition was applied to check and validate if the user is from the correct domain or not and having a specified serial number of the device or not. If devices passed this parameter then the first assessment of security check is passed else traffic is detected and dropped. (a) HIP conditional security parameter.

2nd HIP parameter was configured if the antivirus updated on the remote untrusted devices or not as shown in Fig. 4.

In this HIP test, remote devices were filtered out if the devices have anti-virus was updated or not. If not then traffic detected and dropped.
By following this 2 step process of cloud security malicious traffic is detected of BYOD users.

E. PHASE 2: TEST

During the 2nd phase of the simulation, we have taken BYOD users sitting inside the organization and using personal untrusted devices connecting corporate network through corporate BYOD wireless system.

1) ARCHITECTURE OF THE BYOD FROM INTERNAL NETWORK

During this phase of the research BYOD environment was established using internal corporate network in cluster with multiple branch over MPLS network and corporate head office network.

The architecture used during this research was shown in the Fig. 4.

During the Pre-authentication, traffic was routed through MPLS network from Branch to head office using Getvpn encryption [27] in a secured method [28].

The components used in Fig. 4 during the research mentioned in the table 3 below.

| Index | Components       | Used for                                      |
|-------|------------------|-----------------------------------------------|
| 1     | Firewall         | DMZ segregation firewall DMZ (cisco firewall) |
| 2     | Firewall         | Internet facing checkpoint firewall           |
| 7     | Firewall         | Internet facing checkpoint firewall for BYOD Internet 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            |

IP address schema used during the research was allocated to BYOD users in Fig. 4 as 192.168.x.x and crossing 2 layers of firewall shown in Fig. 4 (index 1 and Index 2). 2nd firewall was used to detect malicious traffic and control.

F. PHASE 3: BYOD USERS OVER INTERNET WITH VPN

This phase simulation was done using VPN services while BYOD endpoint was placed over the internet and cloud VPN services were used for connecting corporate network and malicious activities recorded.

1) ARCHITECTURE BYOD DESIGN OVER INTERNET WITH VPN

During this study, we have focused on the Business Continuity Plan for the organization due to COVID-19 pandemic lockdown and how organization Critical infrastructure requirements got changed suddenly and BYOD becomes more important for the organization. BYOD enablement has taken a remarkable position during COVID-19 situation.

Business enablement using BYOD for the organization during COVID-19 was focused entirely on the enablement of remote VPN services and collaboration approaches.

Many of the organization needs employees to work from home but onboarding BYOD on the corporate network becomes a challenging situation. 2nd challenging situation is even in the existing corporate used remote VPN enablement of all 100% employees becomes critical.

In this study, we analyzed and explored both the objective can be met while major roadblock of this enablement which is the cyber threat is addressed.

The major question to address is how to enable the BYOD users during COVID-19 and enabled detection and control mechanisms of cyber threats.

During the study, we have done the simulation, how BYOD users’ malicious activities can be detected towards the approach to building a Cyber forensic ecosystem for further investigation of suspicious activities.

Also how to enable secure remote vpn services through cloud and back to back traffic comes to the existing private data center.

In this phase we have used Global Protect services as IaaS and Global Protect VPN were used to authenticate users and provide remote access VPN services and performed step by step process as mentioned in Table 5.

During this phase, we have explored the option of how to onboard BYOD users to enterprise networks securely and detect the threat and protect corporate infrastructure.
The architecture used during this simulation as mentioned in Fig. 5.

During this simulation different technology and products used to find the results. Below mention table 6 mentioned the components used during this test and the products used.

Implantation was done with a base line standard configuration as per the description of table 6.

In this case, traffic flow direction was tested as mentioned in table 7.

As mentioned above different directional traffic generated during the test.

Palo Alto global protect [31] VPN services used for this simulation for BYOD users secured onboarding during the covid-19 outbreak. The users were dialing to Palo Alto Prisma [32] cloud where Global Protect VPN services hosted. The service was hosted in GCP (Google cloud platform) [33].

Traffic generated directional flow of traffic as per fig.5a mentioned below.

While Saas Application traffic flow was as mentioned in fig.5b below.

And at last Internet-facing traffic was filtered flow of traffic as mentioned in fig.5c.

Results, analysis of different traffic category was detected during these simulations as mentioned in the Result and Analysis section.

### III. RESULT AND ANALYSIS

As the simulation was conducted with 3 different phases. Results are also analyzed in a different section as Phase 1, Phase 2 and Phase 3.

#### A. PHASE 1 RESULT: DETECTION AND MALICIOUS TRAFFIC FROM INTERNET FACING BYOD USERS

BYOD mobile roaming users completely placed over internet was prime focus area in this section. Results are captured and analyzed in sequence. Different category malicious activities, data leakage, security incident, security compliance was main area while dealing with remotely working users. Detection of

---

**TABLE 5. Sequential process step by step performed.**

| SL No | Procedures                                      |
|-------|-------------------------------------------------|
| 1     | Prisma Access used in GCP                      |
| 2     | Policies used to protect unauthorized used      |
| 3     | Policies for the minimum requirement was as     |
|       | a. User has to be from the test domain         |
|       | b. Users should have very specific malware      |
|       | protection as Symantec was used.               |
| 4     | In case the above cases do not match then      |
|       | disable the access and action triggered as     |
|       | block the user performing any activities.      |
| 5     | Monitor and control                            |

**TABLE 6. Index of the components used in this architecture.**

| Index | Description                                                      |
|-------|------------------------------------------------------------------|
| 1     | BYOD Remote Users authentication traffic to cloud Palo Alto Firewall |
| 2     | Cloud-native Palo Alto Firewall for VPN authentication           |
| 3     | Authentication request to Azure AD for user check               |
| 4     | Cloud Active Directory (Azure AD)                                |
| 5     | Federation service Authentication to Internal Active Directory   |
| 6     | Internal Active Directory                                       |
| 7     | Post Authentication data traffic                                 |
| 8     | Enterprise DMZ firewall                                         |
| 9     | Internal Firewall                                               |
| 10    | Internal Network unfractured                                    |
| 11    | trusted MPLS Cloud                                              |
| 12    | Remote Branches                                                 |
| 13    | Cloud based traffic                                             |
| 14    | Saas based traffic                                              |
| 15    | The direction of cloud exit traffic                             |

**TABLE 7. The direction of traffic simulated.**

| Source            | Destination                  | Traffic type         |
|-------------------|------------------------------|----------------------|
| BYOD users        | Cloud VPN gateway            | Authentication       |
| Cloud VPN Gateway | Cloud AD→Internal AD         | Federated authentication service |
| BYOD users        | Internal Network             | Post authentication data traffic |
| BYOD users        | SaaS application             | Internal cloud hosted services |
| BYOD users        | Internet                     | Any cloud internet services |
malicious traffic was main attention. Data leakage traffic was captured in Fig. 6a.

Assistance of this simulation outcome was data theft which is a major risk [34] for the corporate from BYOD end point was achieved. Fig. 6a shows the traffic category was DLP and detected.

While continuing the simulation one more important category traffic DoS attack which was a major category external threat lead to data breach. DoS attack traffic detection is showing in Fig. 6b.

Further investigation to identify the users and devices was also conducted to back trace the user as shown in result section phase 2.

Continued the test and moved one step ahead for further detection of the end point and found the result of the BYOD end point device level virus status from where malicious traffic triggered for different category as shown in Fig. 6c.

This result also show till the device details of BYOD which was further investigated.

Finally we explored the attack vector, threat factor and event category summary of the complete infrastructure and found the significant details which was beneficial for complete landscape view as shown in Fig. 6d.

This was a significant summary result of the study and further details were also in details per device category.

End of the phase 1 result summarized the security compliance of all BYOD end points, across functionlizes of different technologies used. Results shown in Fig. 6e.

Security compliance dashboard was finally reflecting all security events, top threat, risk and all BYOD devices. This dashboard gives the direction of the security policy across the platform.
B. PHASE 2 RESULT: DETECTION AND MALICIOUS TRAFFIC FROM INTERNAL SEGMENT CONNECTED BYOD USERS

Insiders are treated as trusted users of the corporate but insiders are more vulnerable for the corporate as studied 62% attack is from insiders users [13]. While exploring this option during the research we found most of the malicious traffic generate from inside network to outside network and detected. Logs are collected from the external firewall of the design shown in Fig. 4 index 2. While traffic was encrypted through EoIP [35] tunnel from the corporate network and directly landed in an external firewall, corporate BYOD untrusted devices were connected inside network access point but Fig. 2 index 1 firewall was crossing with encryption and in 2nd firewall, all BYOD traffic was filtered. Using Ethernet-Over-IP Tunnel (EoIP) untrusted mobile device traffic is routed in layer 2 and gateway of the BYOD devices was used in the external firewall (Fig. 4, index 2) so that trusted network gets isolated from untrusted device traffic.

Even though BYOD traffic was securely routed through the corporate network but at the gateway level, all malicious traffic was decrypted and detected.

BYOD users were using the IP address of 172.28.x.x network to access internet post secure authentication. In this research we have explored pre-authentication traffic and all post-authentication traffic was filtered for malicious content. Mentioned in Fig. 6 below malicious contented was detected.

For analysis, internal threat from IP address 172.28.61.127 this BYOD devices generate malicious traffic to BitTorrent Protocol and P2P file sharing primary category.

During the research, internal BYOD generated threat was analyzed so that investigation can be done for the evidence

While one step ahead further logs were analyzed it was found that multiple BYOD device traffic was generating different types of malicious traffic and captured for further investigation as shown in the Fig. 7.

[FIGURE 7. BYOD malicious traffic logs.]

Malicious contents were detected using a checkpoint advance application-layer control blade [36] as shown in Fig. 7 malicious traffic was triggered from 172.28.61.127 and 172.28.4.242 IP address and destined to BitTorrent protocol and P2P category file sharing. Logs were further used during the investigation of the users.

Also, the back trace of the BYOD user was conducted during the research and investigated. This back trace was handled with AAA server where secure certificate-based authentication [14] was done and cisco prime was used during the research to identify the reverse user and investigate.

Identification of the IP to BYOD user who has done malicious activity which was a most critical part. During the simulation, we used the Cisco prime and cisco identity service engine to backtrack. Since the user was connected on wireless Access point so cisco prime logged the IP address with the user and device identity as below.

As captured and shown in Fig. 8, 172.28.61.127 IP address was used by the users having android and mac address 2E:70:8E:93:CF:6A. this shows that IP 172.28.61.127 users connected on the SSID research during the time of malicious activity.

[FIGURE 8. BYOD IP to device identification.]

Historical data of the connectivity and association is also found from cisco prime. Table 8 mention below shows the IP address associated with the users and connected time which matches with the logs to investigate further.

Our next step was to identify the same mac address 2E:70:8E:93:CF:6A authentication and onboarded so that a complete detection mechanism is correlated.

As result captured in Fig. 8 from the Identity service engine was traced to identify the BYOD malicious activity device and the user with mac address 2E:70:8E:93:CF:6A.

Fig. 9 depicts the correlation between the IP address 172.28.61.127 and the test username indrajeet with mac address 2E:70:8E:93:CF:6A with an android device.

Our final step of finding the authentication logs of this device through AAA so that ecosystem gets completed to confirm the users.

In order to confirm this fact, AAA authentication logs was also checked and found the same devices authenticated as mentioned in Table 9.

This authentication message portrays the complete ecosystem of the detection mechanism of the malicious activity.

Finally, we concluded that the malicious activity that happened in the BYOD environment on 24th June’20 which detected in the external firewall was the user of Indrajeet and having BYOD device mac address of 2E:70:8E:93:CF:6A
and had allocated an IP address of 172.28.61.127. The detection process completed with identified malicious users.

Application wise malicious traffic detected as shown in figure below

From inside network 172.28.x.x network to different restricted category destination traffic was generated and logged for the further forensic ecosystem to investigate and which was a continuous process.

| Association Time | Duration | IP Address | User Name | SSID | Protocol | RSSI (dBm) | SNR (dB) | Traffic (MB) |
|------------------|----------|------------|-----------|------|----------|------------|----------|--------------|
| 2020-Jun-24 11:16:43.4 IST | 50 min 49 sec | 172.28.61.127 | Indrjeet | Research | 802.11n | -62 | 32 | 39.1 |
| 2020-Jun-24 12:07:33.5 IST | 50 min 42 sec | 172.28.61.127 | Indrjeet | Research | 802.11n | -48 | 46 | 0 |
| 2020-Jun-24 12:58:16.3 IST | 1 hrs 45 min 38 sec | 172.28.61.127 | Indrjeet | Research | 802.11n | -50 | 49 | 80.7 |
| 2020-Jun-24 14:43:34.8 IST | 3 hrs 18 min 0 sec | 172.28.61.127 | Indrjeet | Research | 802.11n | -49 | 49 | 34.3 |
| 2020-Jun-24 18:01:68.0 IST | 1 hrs 29 min 27 sec | 172.28.61.127 | Indrjeet | Research | 802.11n | -49 | 45 | 0 |
| 2020-Jun-24 11:16:43.4 IST | 50 min 49 sec | 172.28.61.127 | Indrjeet | Research | 802.11n | -62 | 32 | 39.1 |
| 2020-Jun-24 12:07:33.5 IST | 50 min 42 sec | 172.28.61.127 | Indrjeet | Research | 802.11n | -48 | 46 | 0 |

1) PHASE 2 RESULT: DETECTION AND malicious TRAFFIC DESTINED TO INTERNAL BYOD

During this phase, we also analyzed the reverse traffic which is malicious in nature. Traffic was detected as per architecture Fig. 4 index 2 firewall so that all malicious category traffic can be identified. Attack category traffic was detected as shown in Fig. 11 below

This category of traffic was generated from the outside network to a destination of the inside network and detected.

During this exercise, a random malicious IP packet was also captured from the external interface of the external firewall (Fig. 4, index 2) and analyzed using Wireshark logs.
Packet captured on Internal facing firewall and analyzed using wire shark [37] logs and detected.

**C. PHASE 3 RESULT: DETECTION AND MALICIOUS TRAFFIC FROM INTERNET FACING BYOD USERS WITH VPN**

Phase 3 simulation results are captured and analyzed for different categories of traffic. In order to conduct an analysis of different category traffic, Palo Alto Global Panorama was used. This result was captured from Prisma Cloud. All the traffic was inspected in the cloud gateway, full Tunnel mode VPN [38] was used. Since full tunnel mode VPN was used so all traffic detected in a cloud gateway. Any traffic generated from the BYOD endpoint and destined to organization corporate network was inspected in the cloud gateway. 2nd scenario all the traffic generated from BYOD endpoint and destined to the sanctioned application (SaaS-based traffic) was also inspected in Cloud gateway. Subsequently, any traffic destined to Internet destination was also inspected in Prisma cloud gateway.

Threat landscape was observed and captured the logs as mentioned in Fig. 13.

The result shows total of 6.06 K hit was there which was spyware category, whereas vulnerability was 201.09K during 30 days period and virus attack was 1.75K

DNS security threat which is a major threat today and root of the threat [39] was also well detected and inspected which was spyware category. DNS Security opens the path for legitimate [40] traffic for the attack which was an important test conducted and traffic inspected in this phase.

And below figure shows the landscape of DNS security where 5.96K traffic was only Spyware DNS security category.

Below was the threats which was inspected and blocked From phase 3 simulation all the traffic destined to the Internet from BYOD end point devices are inspected and this was demonstrated that malicious traffic was detected with all different level of severity in place. This traffic was further logged in Cortex for data lake for a further forensic investigation of threat and other malicious activities. During COVID-19 lockdown situation while employees are required to onboard using the BYOD endpoint in the corporate network, this method of onboarding shows a significant result of developing a secured model of cyber threat detection mechanism which further helped to build cyber forensic eco-system for the organization for threat handling.

**D. BYOD MALICIOUS TRAFFIC PATTERN**

While the different category of the restricted traffic was detected during the research it was observed a large amount of data was generated in a different category and overall BYOD network infrastructure build to detected those malicious activities and control.

Different attack pattern risk wise, category wise are summarized in Fig. 14. This broad categorization was used for
defining the policy of the organization. This security policy implementation in the organization finally used for the secured BYOD environment.

By detection of these risks and attacks which were critical for the organization approached the model of policy and build a secured cyber forensic ready BYOD environment.

IV. DISCUSSION

A secured Cyber Forensic BYOD ecosystem needs an advanced level of malicious activity detection mechanism. The initial objective of this research was to detect malicious traffic from BYOD users. In this study we have analyzed detection mechanisms and then deploy proper security control so that internal infrastructure risk can be identified. We have detected the malicious traffic using a cloud firewall placed between the cloud access broker and on-prem access connector and also in-depth investigation of the on-prem firewall.

The subsequent objective was to protect the internal infrastructure then also Forensic investigation of BYOD malicious traffic. Using Cloud firewall and DMZ Access connector untrusted BYOD malicious traffic was protected to enter inside organization internal network. The most critical task is the detection of Cyberattack in the BYOD environment which was addressed and in detailed investigation process and mechanism developed using checkpoint technology and Palo Alto.

From diversified study in this extent, this was concluded that the major security risk of the country is BYOD security [41], BYOD also carries danger if control of security if it is not implemented and if infra is not forensic ready then obviously “Bring your own danger” [42].

During this research 3 phase simulation was conducted for result analysis from different directions of traffic. Subsequently, a different category of attack and malicious activities were documented as below

| Phase | BYOD setup | Detection mechanism | Malicious activity detection |
|-------|------------|---------------------|----------------------------|
| Phase 1 | In this phase, BYOD users were kept in remote place over internet to connect corporate network without VPN | Malicious activity detected using cloud Security | Yes |
| Phase 2 | In this phase BYOD users kept inside the corporate network and connected over wireless | Malicious activity detected using on-prem security | Yes |
| Phase 3 | In this BYOD users kept in remote over internet without VPN and cloud services | Malicious activity detected using On-prem 3 layer security | Yes |
As mentioned above 3 different phases of the simulation were conducted to conclude the detection process of suspicious activities. Post simulation of different types of BYOD onboarding process from different direction to the corporate network, derived a model of standard process of BYOD environment as mentioned in Fig. 15. Which build a secured cyber forensic eco system

End of all 3 phase simulation we also derived a systematic process for BYOD secured ecosystem development modes as mentioned in Fig. 16.

V. CONTRIBUTION

Detection of malicious traffic from BYOD environment was the prime objective of the research. Apart from this COVID-19 pandemic situation has changed the entire traditional model of the working environment and turned to work from the home alternate method of working environment. BYOD malicious traffic of Cyber security risk concludes that there is a need for cyber confidence alternate method of the working environment and how to build a secured model of BYOD environment with cyber forensic capability.

A very important contribution of this research was the detection of malicious traffic from BYOD untrusted users to protect the corporate network. While organizations continue to enable the BYOD services for today’s ongoing demand but onboarding of untrusted devices is risky. A complete ecosystem of detection of malicious traffic and control of this malicious traffic is a fundamental need. This research has enabled the way forward for enabling forensic investigation for BYOD traffic proper detection mechanism is required and the research was contributed in defining the mechanism of detection and protection of BYOD malicious traffic using different security control mechanism. Checkpoint and Palo technology was used to detect malicious contents and result analyzed.

VI. FUTURE RESEARCH

This research has given an important contribution in developing a model of detecting malicious activities in BYOD environment but this research indicates a complete end to end eco-system is required to build for the forensic investigation process to complete for cybercrime mechanism. Building a cyber-forensic BYOD secured infrastructure can be explored further with advanced level security in place.

VII. CONCLUSION

An impending crisis situation in BYOD cyber forensic ecosystem is a unique mechanism of detection of malicious activities which is a core component. A continuation of current trends of detecting suspicious activities abstraction was in requirement to build an advanced technique. This paper focused towards a new abstraction with more efficient technique in practical approach for detecting malicious activities in BYOD environment.

The aim of this research was to build an advanced level detection mechanism and control of malicious activities. By using threat extraction mechanism using checkpoint sandblast and cisco ISE for AAA during the research and also Palo Alto was used, by using all these technology and tools, this was possible to build a secured BYOD infrastructure where malicious activities are detected and investigated. By using certificate based AAA authentication model with a combination of advance security technology every users can be back traced and evidence of every activities can be analyzed for further investigation. This research concludes mechanism of Detection of malicious activities by insiders as well as outsiders and protect the organization critical infrastructure. 2nd part of the research was to control the BYOD insiders’ malicious traffic and build a progressive level mechanism to build a cyber forensic ecosystem so that detection, control, and investigation correlates with logs and artifacts. this was also achieved. Post analysis of this experimental study and simulation, it is observed that the proposed method increased to develop more advance BYOD forensic ecosystem. Furthermore this mechanism is also beneficial not only to detect the malicious activities and attack but also it control the attack in today’s advance threat trend. In Future work we will consider to next level of this research of building advance level forensic eco-system.

Current diversity of the research with multi-vendor community environment, the outcome is not sufficient to combat with today’s threat landscape. Security OEM need to adopt a collaboration approach and work towards developing a compatible standard ecosystem to protect organization from attack.

REFERENCES

[1] *Global Risks 2019: Insight Report*, Weltwirtschaftsforum Zurich Insurance Group, Zürich, Switzerland, 2019.
[2] WHO Director-General’s Opening Remarks at the Media Briefing on COVID-19—11 March 2020. Accessed: Apr. 20, 2020. [Online]. Available: https://www.who.int/dg/speeches/detail/who-director-generals-opening-remarks-at-the-media-briefing-on-covid-19—11-march-2020
[3] World Economic Forum. 'Here’s What Lockdown Looks Like Around the World.' Accessed: Apr. 20, 2020. [Online]. Available: https://www.weforum.org/agenda/2020/04/coronavirus-lockdowns-global/
[4] *Global Risks 2019: Insight Report*, Weltwirtschaftsforum Zurich Insurance Group, Zürich, Switzerland, 2019.
[5] World Economic Forum. *The Global Risks Report 2020*. Accessed: Apr. 20, 2020. [Online]. Available: https://www.weforum.org/reports/the-global-risks-report-2020/
[6] ‘As the Number of Remote Workers Rises, Cisco Supports Customers With Expansion of Free Security Offerings—Cisco Blogs.’ Accessed: Apr. 23, 2020. [Online]. Available: https://blogs.cisco.com/security/cisco-expands-free-security-offerings-to-help-with-rise-in-remote-workers
[7] W. Largent. Threat Roundup for April 10 to April 17, Accessed: Apr. 23, 2020. http://blog.talosintelligence.com/2020/04/threat-roundup-0410-0417.html
[8] A. Rao and C. T. Solutions, “Combating cybersecurity challenges with advanced analytics,” Digit. Syst., p. 24.
[9] O. Johnson. (Apr. 20, 2020). Cognizant Left With ‘No Good Options’ After Maze Attack: Security Expert. Accessed: Apr. 23, 2020. [Online]. Available: https://www.cnbc.com/2020/04/20/cognizant-left-with-no-good-options-after-maze-attack-security-expert
[10] H. Shetty, L. Unden-Farboud, and P. Arriandiaga, “Competitive landscape: Managed mobility services,” Tech. Rep., p. 20.
(11) 94% Enterprises Will use IoT by end 2021: Microsoft Report. Accessed: Aug. 8, 2019. [Online]. Available: https://www.livemint.com and https://www.livemint.com/technology/tech-news/94-enterprises-will-use-iot-by-end-2021-microsoft-report-156516549842.html

(12) B. Tokuyoshi, “The security implications of BYOD,” Netw. Secur., vol. 2013, no. 4, pp. 12–13, Apr. 2013, doi: 10.1016/S1535-4858(13)70050-3.

(13) J. Collie, “A strategic model for forensic readiness,” Athens J. Sci., vol. 5, no. 2, pp. 167–182, Jun. 2018, doi: 10.30958/ajs-5-2-4.

(14) M. I. Ali and S. Kaur, “Detection and control of malicious activity and digital forensic in BYOD,” Tech. Rep., p. 7.

(15) K. AlHarthy and W. Shawkat, “Implement network security control solutions in BYOD environment,” in Proc. IEEE Int. Conf. Control Syst., Comput. Eng., Penang, Malaysia, Nov. 2013, pp. 7–11, doi: 10.1109/ICCSCE.2013.6719923.

(16) K. AliHarthy and W. Shawkat, “Implement network security control solutions in BYOD environment,” in Proc. IEEE Int. Conf. Control Syst., Comput. Eng., Penang, Malaysia, Nov. 2013, pp. 7–11, doi: 10.1109/ICCSCE.2013.6719923.

(17) P. K. Gajar, A. Ghosh, and S. Rai, “Bring your own device (BYOD): Security risks and mitigating strategies,” Tech. Rep., 2010, p. 9.

(18) K. Joshi, M. Pathak, S. Jose, S. Dahiya, and S. Jose, “(71) applicant: Gigamon Inc., Santa Clara, CA (US),” Tech. Rep., p. 18.

(19) M. M. Singh, S. S. Siang, O. Y. San, N. H. A. H. Malin, and A. R. M. Shariff, “Security attacks taxonomy on bring your own devices (BYOD) model,” Int. J. Mobile Netw. Commun. Telematics, vol. 4, no. 5, pp. 1–17, Oct. 2014, doi: 10.5121/jmict.2014.4501.

(20) F. Jamal, M. T. Abdullah, A. Abdullah, and Z. M. Hanapi, “Enhanced bring your own device (BYOD) environment security based on blockchain technology,” Int. J. Eng., vol. 7, no. 4 and 31, pp. 74–79, 2018.

(21) F. Jamal, M. T. Abdullah, A. Abdullah, and Z. M. Hanapi, “BYOD authentication process (BAP) using blockchain technology,” J. Adv. Res. Dyn. Control Syst., vol. 10, no. 11, p. 8, 2018.

(22) V. R. Kebande, N. M. Karie, and H. S. Venter, “A generic digital forensic readiness model for BYOD using honeypot technology,” in Proc. IST-Africa Week Conf., Durban, South Africa, May 2016, pp. 1–12, doi: 10.1109/ISTAFRICA.2016.7530590.

(23) A. Marotta and M. McShane, “Integrating a proactive technique into a holistic cyber risk management approach,” Risk Manage. Insurance Rev., vol. 21, no. 3, pp. 435–452, Dec. 2018, doi: 10.1111/rmir.12109.

(24) N. Serketzis, V. Katos, C. Ilioudis, D. Baltatzis, and G. Pangalos, “Improving forensic triage efficiency through cyber threat intelligence,” Future Internet, vol. 11, no. 7, p. 162, Jul. 2019, doi: 10.3390/fi1107162.

(25) D. A. Flores, F. Qazi, and A. Jhumka, “Bring your own disclosure: Analysing BYOD threats to corporate information,” in Proc. IEEE TrustCom/BigDataSE/ISPA, Tianjin, China, Aug. 2016, pp. 1008–1015, doi: 10.1109/TrustCom.2016.0169.

(26) “Group encrypted transport VPN (get VPN) design and implementation guide,” Tech. Rep., p. 165.

(27) I. Ali and S. Kaur, “Detection and control of malicious activity and digital forensic in BYOD,” Tech. Rep., p. 7.

(28) M. Ratchford, P. Wang, and R. O. Sheit, “BYOD security risks and mitigations,” in Information Technology—New Generations, vol. 558, S. Latifii, Ed. Cham, Switzerland: Springer, 2018, pp. 193–197.

(29) M. P. Souppaya and K. A. Scarfone, “Guide to enterprise telework, remote access, and bring your own device (BYOD) security,” Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-46r2, Jul. 2016, doi: 10.6028/NIST.SP.800-46r2.

(30) Palo Alto Networks | TechDocs Home. Accessed: Jun. 28, 2020. [Online]. Available: https://docs.paloaltonetworks.com/PrismaAccess.

(31) Palo Alto Networks | TechDocs Home. Accessed: Jun. 28, 2020. [Online]. Available: https://docs.paloaltonetworks.com/prisma/prisma-access.

(32) S. Challita, F. Zalila, C. Gourdin, and P. Merle, “A precise model for Google cloud platform,” Tech. Rep., 2018, p. 183.

(33) A. Al-Bataineh and G. White, “Analysis and detection of malicious data exfiltration in Web traffic,” in Proc. 7th Int. Conf. Malicious Unwanted Softw., Fajardo, PR, USA, Oct. 2012, pp. 26–31, doi: 10.1109/MALWARE.2012.6461004.

(34) “Monitoring and validating mobility,” Tech. Rep., p. 4.

(35) Application Control Software Blade. Accessed: Jun. 26, 2020. [Online]. Available: https://sc1.checkpoint.com/documents/R80.40/Web/AdminGuides/EN/CP_R80.40_NextGenSecurityGateway_Guide/Content/Topics-FWG/Application-Control-Blade.htm.

(36) Wireshark - Go Deep. Accessed: Oct. 6, 2019. [Online]. Available: https://www.wireshark.org/.

(37) D. I. Wolinsky et al., “On the design and implementation of structured P2P VPNs,” Tech. Rep., p. 16.

(38) DNS Security and Services | Akamai. Accessed: Jun. 30, 2020. [Online]. Available: https://www.akamai.com/us/en/solutions/security/dns-security-services.jsp.

(39) “Cyber security report 2020,” Tech. Rep., 2020, p. 8.

(40) 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, Switzerland: Springer, 2019, pp. 252–262.

(41) P. Beckett, “BYOD—popular and problematic,” Netw. Secur., vol. 2014, no. 9, pp. 7–9, Sep. 2014, doi: 10.1016/S1353-4858(14)70090-X.