Hindawi
Security and Communication Networks
Volume 2021, Article ID 6664426, 19 pages
https://doi.org/10.1155/2021/6664426

WILEY | Hindawi

Research Article

Next-Generation Digital Forensic Readiness BYOD Framework

Md Iman Ali[1] **and Sukhkirandeep Kaur**[2]

[1]*Department of Computer Application, Lovely Professional University, Phagwara, Punjab, India*
[2]*Department of CSE, Lovely Professional University, Phagwara, Punjab, India*

Correspondence should be addressed to Md Iman Ali; mdiman@rediffmail.com

Received 31 December 2020; Revised 21 January 2021; Accepted 4 February 2021; Published 22 March 2021

Academic Editor: Manjit Kaur

Intel's "Bring Your Own Device" (BYOD) adoption quickly became popular as an alternative workplace solution strategy. It enables employees to use their personally owned devices to perform business activities, leading to increased productivity and employee satisfaction. However, BYOD also brought associated risks because of exponential growth in the number of cybersecurity incidents due to which business ecosystem gets disrupted and fragmented. Although several methods and mechanisms have been developed and adopted to mitigate the risk associated with BYOD, they still represent a challenge as corporate network gets exposed to inherent threats caused by the BYOD threat landscape. This work demonstrates especially two key aspects: The first focuses on how to detect and protect BYOD environment from an advanced level attack which cannot be detected by traditional tools and techniques even though available tools are quite effective. Before the attack and damage to the critical infrastructure due to BYOD threat, a strategy was indeed the key requirement for detecting attacks and protecting the environment. The second part of the research focuses on conducting forensic investigation model and developing a new approach by providing a reliable forensic investigation infrastructure to find digital evidence and detect the source of attack. This research work concluded with two different novel strategic ideas. The first part contributes to a new method of detecting and protecting against malicious activities which cannot be otherwise detected and protected by traditional security technology like IPS, IDS, AntiBot, or AntiVirus. The proposed technique compared to the existing methods led to a significant contribution to the identification of threats before an attack takes place. The second part of the research contributes to the defining of a new approach of the next-generation digital forensic readiness (NG-DFR) model in order to build a cyber forensic ecosystem so that cyber secured BYOD environment can be enabled safely.

1. Introduction

Bring Your Own Device (BYOD) is basically the consumerization of information technology (IT) where employees use their personal devices in the corporate networks. It helps the organization to save the cost and increases employee productivity and engagement. Adopting BYOD technology in enterprise leads to an increase in business productivity and enhances collaboration and business agility.

Bring Your Own Device (BYOD) becomes a rule rather than an exception. Technology transformation is the key role of every CIO and IT leader of any organization. As per the study of Gartner, BYOD users will get increased by 75% by 2022 [1] from 35% in 2018. By 2021 [2], maximum organizations are expected to use IoT; approximately 94% of the organizations will adopt IoT as per Microsoft report. During the COVID-19 global pandemic situation, demand for BYOD has even increased exponentially.

The BYOD infrastructure provides Internet access to the employees, while employees being trusted users access the enterprise infrastructure, which is intended to be secured. Guest user access is also one of the features of BYOD to provide access to the visited partner/guest using the self-registration portal or sponsored portal. During the initial stage of the BYOD solution adoption, most of the organizations did not give access through corporate network due to involved security risks. However, in the later stage, organizations started moving towards a positive direction

realizing that personal mobile devices are an integral part of employees' daily life. As BYOD connects untrusted external devices in the corporate wireless network infrastructure, increase in cybersecurity risks and data leakage incidents are observed. Malicious activities can be performed using BYOD. Unmanaged devices might not be following the standard security practice and may not follow the line of defense against malicious content [3]. A study concluded that 62% of digital incidents are triggered by inside users either intentionally or unknowingly [4]. Using BYOD services, users can try to get access to internal network and cloud network, and perform malicious activities, and damage the potential data which can cause the reputation loss of the organization. Data theft, shadow IT, and cybersecurity constitute a major concern in BYOD. Installing malware in BYOD and connecting to the Internet can also lead to serious damage and are a major security risk. While implementing the BYOD legal approach of the mitigation cannot be overlooked [5], every stage of the BYOD security policy should be always in line with protecting the internal network, data, and application. BYOD system has become a huge security risk [6]. Accessing corporate infrastructure using BYOD devices which may be owned by employees, suppliers, or partners makes corporate data protection a major concern for the organization; at the same time, isolating personal data is a need for employee privacy. In a study, the BYOD security impact assessment conducted for the airport smart system stated that compromised BYOD devices can have an impact on airport system integrity and availability [7]. Security breaches are more in terms of the network infrastructure where BYOD service is offered to employees, partners, and staff.

Cyberattack and security risk in airport security is a major risk of the country [8] due to BYOD. BYOD might become "bring your own danger" [9] if proper security control is not implemented and if the solutions do not include forensic investigation after crime.

Due to vulnerability, cyber-attacks have grown periodically. According to CVE [10], Figure 1 represents the growth of vulnerabilities in years. Increase in vulnerability has also increased the attacks.

DFR (digital forensic readiness) in BYOD infrastructure is one of the models that detect attackers' activities and behavior using honeypot, a deception technology. Extensive research has been conducted to improve the approach of DFR and CTI (cyber threat intelligence) to conduct a digital forensic investigation and to reduce the time and cost. Up to 90.73% [11] accuracy level was achieved in analyzing the root cause after an incident.

According to Juniper Survey, 80% of BYOD devices will be unprotected. There is a need for digital forensic infrastructure in BYOD technology to provide security. Lack of a proactive security model in BYOD architecture can cause digital forensic investigation. A large-scale clustering deployment of BYOD infrastructure needs an advanced model of digital forensic readiness infrastructure for the practice of detection and investigation [12].

Internet users are increasing exponentially by using IoT/BYOD in every organization, public environment, and smart city environment. Cyberterrorism is defined as the intentional use of a computer or network communication device using public networks to destruct the critical public and private infrastructure for personal objectives which may be political or ideological. The government and public/private sector must gear up to fight against this major crime. Cybercrime rates are also exponentially growing, and this is a challenging area to handle and investigate after an incident. Government of India has taken an initiative to enhance the infrastructure of the National Cybercrime Forensic Laboratory (NCFL) and started a new project called Cyber Prevention, Awareness & Detection Centre (CyPAD) as stated by Union Home Minister on the 18th of Feb 2019 [13]. Union Home Minister has pointed out that cybercrime has become a big challenge to handle. Different questions arise: How governments or private organizations will handle such big cyber forensic investigation and cyber fraud management in smart city environment where IoT users are in large numbers or BYOD users are increasing every day? Who will do this investigation? How those crimes will be handled? How to get the crime activity logs of BYOD/IoT users?

These questions can be addressed by developing and implementing a cyber secured BYOD infrastructure. After an attack, there is a need for forensic investigation in BYOD. Major components in digital forensic investigation are [14]

Computer forensic

Network forensic

Database forensic

Mobile forensic

Digital forensic or cyber forensic will ideally include the components [15] (a) humans, (b) digital evidence, and (c) process, which act as a reference point. After a cyber-attack analysis, event reconstruction, with reproducible and verifiable results, is an inline requirement for legal action in digital forensic investigation [16]. BYOD has all those components to be covered in forensic investigation. Threat finding after an incident and source of attack [8] finding are requirements in forensics; for example, a novel study was conducted for identifying human behavior in an automated way based on handwriting [17].

On the other hand, the cloud adoption rate is expected to be 83% by 2020 [18]. This increased rate of cloud adoption has increased the demand for BYOD at a much larger rate. All organizations are adopting cloud services for different applications and roaming user services, since the increased demand for working anywhere by any device has increased the BYOD demand. At the same time, BYOD security and cyber forensic investigation from enterprise network and cloud network are important concerns that need to be taken care of.

There is a serious need for BYOD forensics as BYOD devices are the most critical component in forensics and the source of evidence [19]. Due to the increased cyber incident

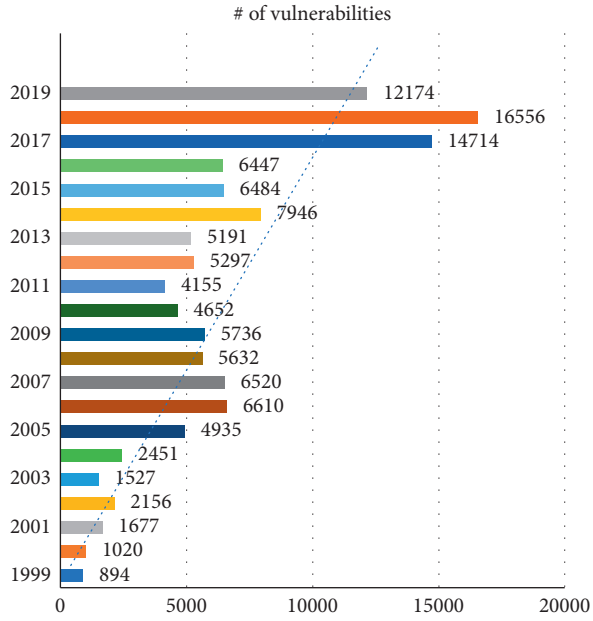


Figure 1: Vulnerabilities by year (CVE).

landscape, collecting, preserving, and analyzing digital evidence after an incident and presenting the analysis with integrity are required.

This paper is organized as follows: Section 2 discusses the related work, followed by design and methodologies in Section 3 and then results in Section 4. Comparison and analysis are provided in Section 5. The proposed new model of NG-DFR is explained in Section 6. Section 7 concerns NG-DFR model ecosystem. The discussion is covered in Section 8, contributions of the research in Section 9, future research areas in Section 10, and conclusion in Section 11.

2. Related Work

Most of the research in this area is conducted from the Golden Age of digital forensics (1997–2007) till today, which is not sufficient to complete the analysis as there was a need for a standard, modular [20] approach to digital forensic. Since new technologies are adopted, the deployment approach is also changing and there is no single mitigation technique [21] as methods of attacks keep on changing. Therefore, continuous evolvement in forensic technology is required as stated in a study by Deloitte [22]. There is no single agreed upon digital forensic process that has been developed [23]. Some of the existing methods and techniques are listed below.

2.1. Honeypot Technology. Deception technology honeypot has been explored to detect threats in BYOD infrastructure in 2016. This opens the way for doing root cause analysis after an incident [12]. An improved extended study of a generic digital forensic readiness model for BYOD using honeypot technology [12] was again conducted in 2019 where a Threat Intelligence Platform is used to detect the incident, and accuracy has been analyzed [11]. Using audit logs of malicious activities collected from the Threat Intelligence Collector, accuracy has been analyzed and found to be 90.73%, 96.16%, and 93.71% [11]. Subsequently, honeypot was integrated with cyber risk management process of five preparedness mission areas of FEMA (Federal Emergency Management Agency) [24].

2.2. Cryptographic Blockchain Method of Forensics. The cryptographic blockchain authentication process has been studied where the record-keeping system has been used for secure authentication of BYOD users. Evidence collection for forensic investigations has also been covered using records [25]. Furthermore, the digital method of record-keeping systems has been used for the multifactor authentication process [25]. This ledger makes an easier way to conduct digital evidence investigation after the crime/malicious activity, for example, image haze removal technique [26], forward mechanism, or reverse mechanism in dual-tree complex wavelet transform (DTCWT) [27]. Using advanced intrusion detection and distributed ledger technology in the IoT environment by identifying malicious activity and finding the source of the attack, storing the digital evidence is explored so that digital evidence can be collected to conduct a digital investigation [28].

2.3. STRIDE Based Threat Model. STRIDE [29] based BYOD threat model is proposed and analyzed threat interaction in BYOD. BYOD internal and external threat interaction with the corporate network are analyzed so that security and forensic threats in BYOD can be understood. Reverse adoption of encryption using the Group Encrypted Transport VPN (GETVPN) method of BYOD traffic was a novel approach to detecting malicious activities and to reducing threats. Therefore, the forensic analysis mechanism was analyzed for internal and external traffic threats [30].

2.4. Smart City IoT Cloud Data Security Forensics. Data security on the cloud is also an important aspect to be considered as stored data in the cloud does not have enough control. Since cloud data is not an enterprise control data center, so data accessed by unauthorized entities is a risk. Data integrity is an important parameter for postincident forensic analysis. Forensic analysis and finding out the root cause constitute the important view that has been highlighted. Artificial intelligence is also one of the major areas that have been pointed out in this study. The identification of security threats is studied in [31].

2.5. IoT Mobile Forensics. Smartphone IoT devices traces were used to find the logs of the incident for forensic investigation. Extracting the logs from IoT devices and analyzing logs captured with Wireshark for finding out digital evidence constituted one of the approaches [32]. Using smartphone devices, collecting the stored logs from the smartphones, and reconstructing the event of crime are very useful case studies done in DFRSW (Digital Forensic Research Workshop). Retrieving the information from digital

IoT devices and analysis of using multiple tools like Wireshark [33] were important findings of digital evidence of the crime [34].

2.6. Integration of Digital Forensics and Forensic Science. The task of collecting digital evidence from a dynamic IoT environment is very complex. Due to a lack of proper tools and techniques, the process becomes very challenging [35]. An important study was conducted regarding the integration of different forensic sciences to build a smart ecosystem of forensic science [36]. While various mechanisms are implemented to reduce security attacks, in some cases image processing reduces the computation speed which has also been addressed in the nondominated genetic algorithm [37]. A powerful digital forensic ecosystem can be created in case of a collaborative effort of different tools, technologies, and cyber laws, and forensic experts can integrate all together.

As per an IBM study in 2018, 77% of organizations do not have a consistent cybersecurity incident response plan (CSIRP) [38], even after the General Data Protection Regulatory (GDPR) has been in effect since May 2018 [39]. On average, it takes 23.6 hours [40] to address cybercrime aftermath. This indicates that there is a serious need for advanced level cybersecurity response systems, cyber defense mechanisms, and cyber forensic mechanisms.

If BYOD cyber forensic mechanism can be developed in such a way that the incident can be analyzed to detect the crime with sufficient evidence, then BYOD cyber forensic ecosystem can be a more reliable environment for the organization.

This study has shown a flagrant result of BYOD malicious activity forensic analysis which can be helpful for organizations to implement cyber defense and cyber forensic ecosystem in the BYOD environment.

2.7. Wireless Drone Forensic Readiness Model. The wireless forensic readiness model was explored with a dedicated forensic server with drone architecture in the year 2011. Packet decryption and Wireshark analysis were done to identify the attack [41], and the collection of digital evidence was explored. After collection of logs, analysis of wireless LAN traffic using NetWitness [23] was another approach explored to conduct a digital forensic investigation.

As discussed above, a different BYOD cyber forensic model has been explored in various tangents, but due to exponential increase of cyber-attack tools and technology, there is a definite need for further development in this area. Hence, the objective of this research is to first secure the BYOD infrastructure using traffic encryption and second develop BYOD forensic investigation using Check Point SandBlast.

3. Cyber Forensic Model: NG-DFR

3.1. High-Level Digital Forensic Readiness BYOD Model. This section presents a high-level digital forensic readiness model. An advanced level of the next-generation digital forensic readiness model is projected. This study has been conducted to detect the cyber-attack, protect infrastructure from threat, and develop a postincident forensic investigation process. As honeypot technology for digital forensic readiness (DFR) [12] is not sufficient and large-scale evidence finding technique was required, the deception technology has been used for digital forensic readiness. As the components of digital forensic or cyber forensic investigation include [15] (a) humans, (b) digital evidence, and (c) process, the model of the advanced digital forensic model needs to include all these parameters. After an incident, finding the threats and tracing the source of attack [8] become a major requirement, and prediction of future attacks based on the current attack is also important, for example, in an engine where future flow demands are based on the current flow [42]. Major components included in this study are represented in Figure 2.

DFR model includes people, process, technology, digital forensic infrastructure, and law enforcement.

3.2. Detailed DFR Model Architecture. The architecture for BYOD in this study was done as per standard design. Multiple OEM products are used. Initially, the BYOD setup was implemented for normal Internet access using the corporate wireless infrastructure.

The same wireless infrastructure is used for corporate wireless and BYOD services. Identity Service Engine [43] was used for authentication and back-to-back user identity was used as Microsoft Active Directory. Table 1 shows the components used during the research.

Components used for testing authentication traffic between branch locations and a central location are represented in Table 2, followed by additional forensic/investigation components used during the research for threat hunting and analysis in Table 3.

3.2.1. Implementation of BYOD Architecture. BYOD architecture was established to initiate the traffic from 2 different sources.

The first category of the BYOD traffic is mentioned in Table 4.

In this research, we conducted 2 different scenarios of BYOD forensic traffic analysis.

(a) Scenario 1. Analysis with Check Point SandBlast: Figures 3 and 4 show BYOD architecture and overall traffic flow with sandblasting as a forensic analysis mechanism.

The index used in Figure 3 for the demonstration is mentioned in Table 5.

(b) Scenario 2. Analysis with Palo Alto Forensic Cortex and cloud instance for BYOD forensic analysis: In this scenario, we conducted an analysis of BYOD forensic traffic with Palo Alto Cortex.

Figure 4 shows additional components used in the test.

The additional components used in the second scenario are presented in Table 6.

During the research in the second scenario, additional components used for BYOD traffic forensic analysis are Cortex of Palo Alto network and Palo Alto 820 as threat prevention, and also Palo Alto Cloud for threat management was used.

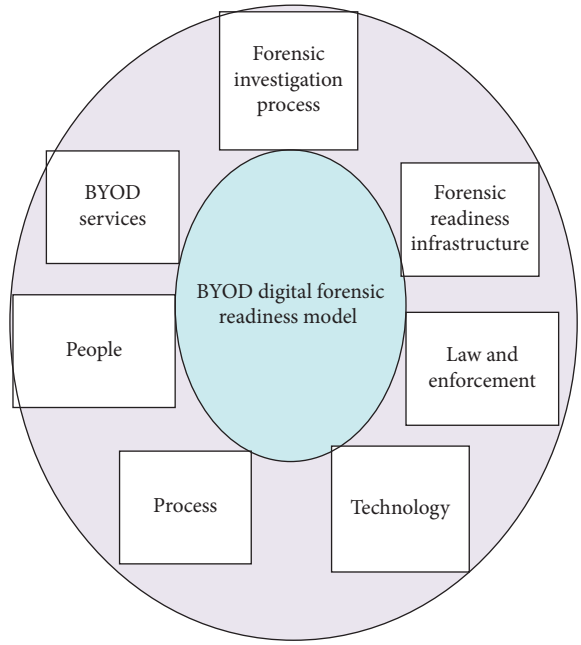


Figure 2: Digital forensic readiness (DFR) model components.

Table 1: Components used to set up the BYOD infrastructure.

Seq#	Product name	Make	Model	Usage
1	ISE (Identity Service Engine)	Cisco	SNS-3495-K9	AAA server
2	Internal firewall	Cisco	ASA5516-FPWR-K9	DMZ firewall
3	Access point	Cisco	AIR-AP4800-D-K9	Access point
4	External firewall	Check Point	CPAP-SG4400-NGFW	External firewall
5	Anchor controller	Cisco	AIR-CT5520-K9	BYOD guest controller
6	Foreign controller/mobility controller	Cisco	C9800-40-K9	Master wireless controller
7	Active Directory	Microsoft		For user database
8	Router	Cisco	ISR 4431	Routing
9	BYOD devices	Different mobile, laptop	Android/iPhone	Testing BYOD devices
10	Internal network endpoint	Lenovo	Laptop	For trusted zone device
11	Log management	Check Point	CPAP-SM225	For traffic log management

Table 2: Components for BYOD traffic.

Sl. no.	Components	Purpose
1	MPLS connectivity	Traffic flow from branch to central location
2	Internet link	BYOD Internet traffic exit

Table 3: Components used for forensic traffic analysis.

Sl. no.	Forensic components	Use
1	ISE	For authentication logs
2	Check Point Forensic Blade	For forensic traffic analysis
3	Check Point SandBlast	For threat hunting
4	Wireshark	Logs analysis

3.2.2. Authentication Mechanism and Onboarding Process of BYOD Users. Authentication and onboarding secured mechanism is used with certificate-based authentication [43]. During the study, for authentication procedures and traffic flow for authentication, ports are allowed on the DMZ firewall.

Table 4: BYOD traffic source/destination.

Sl. no.	Source	Destination	Description
1	Local BYOD users	Internet	Without MPLS network
2	Remote branch BYOD traffic	ISE for authentication	Across MPLS network

The ports opened on the DMZ firewall during the study index 6 (Figures 3 and 4) for communication purposes of BYOD management traffic are listed in Table 7.

3.2.3. Cyber Defense Ready BYOD Infrastructure. The proactive approach of implementing BYOD was followed so that malicious activities can be detected and protected against to reduce the threat and risk. Implementing

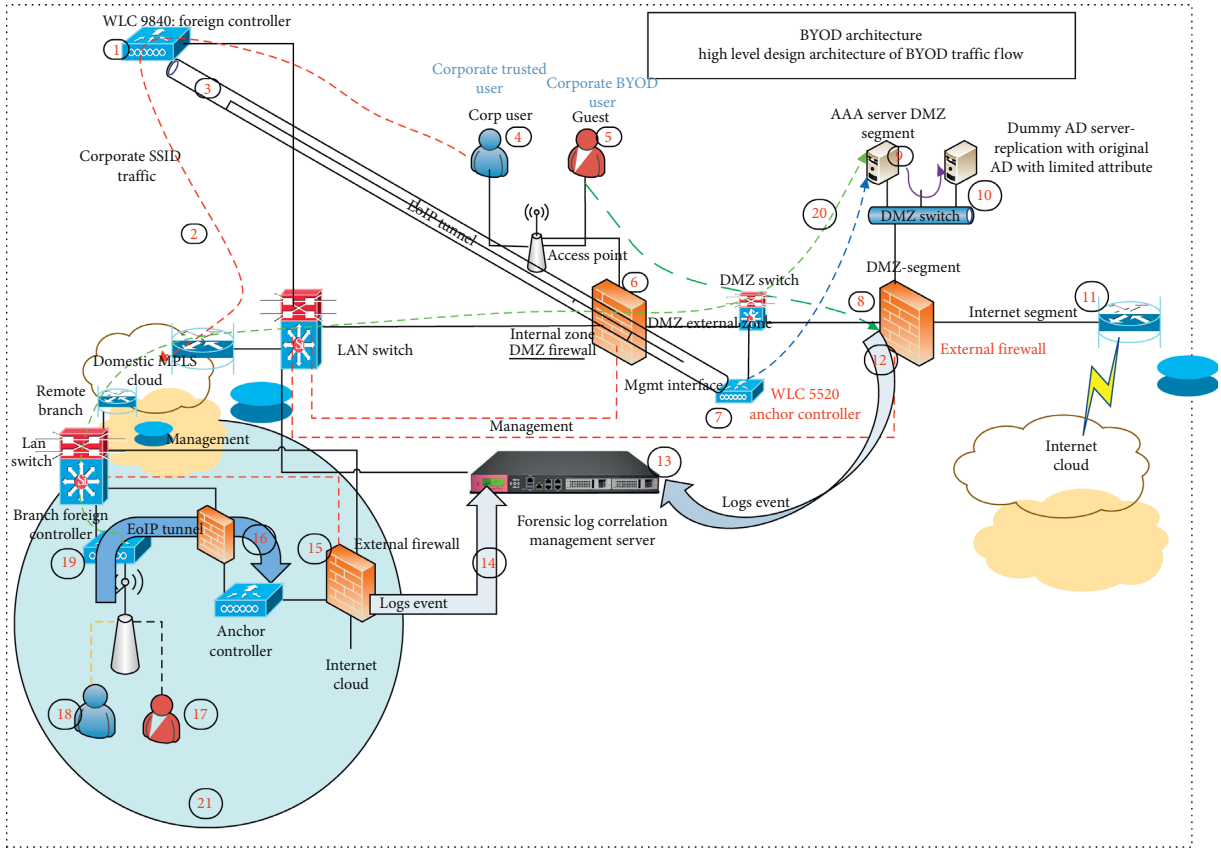


Figure 3: High-level BYOD traffic flow architecture.

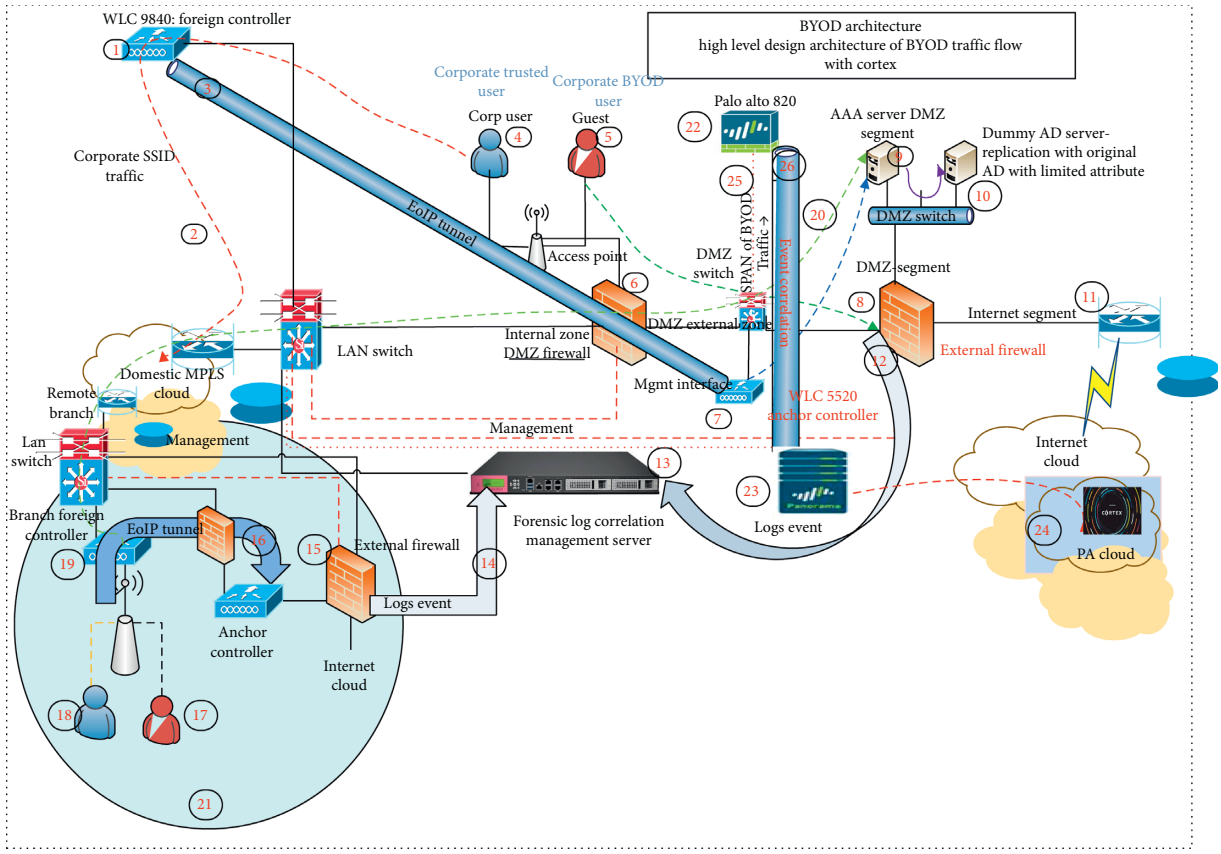


Figure 4: BYOD architecture with Palo Alto Cortex.

Table 5: The index used in Figure 3.

Index	Description
1	Wireless LAN controller
2	Authentication traffic from branch to AAA server
3	Ethernet over IP (EoIP) tunnel between foreign controller and anchor controller
4	Corporate users (non-BYOD)
5	BYOD untrusted users
6	DMZ segregation firewall
7	Anchor controller (guest controller)
8	External firewall
9	AAA (authorization, authentication, accounting) server for BYOD authentication
10	Active Directory for user identity
11	External Internet router
12	Traffic logs from gateway to management server for activity logs
13	Management server (log management)
14	Traffic logs from branch to central management server
15	Branch external firewall
16	EoIP tunnel
17	Branch BYOD users
18	Branch trusted users
19	Branch foreign controller
20	Authentication traffic from branch to central site AAA server
21	Branch/remote location

GETVPN for segregation and encryption of authentication traffic reduced the number of threats over MPLS [44]. Traffic was encrypted and segregated using GETVPN over MPLS which reduced the initial risk of the infrastructure and protected internal infrastructure.

3.2.4. Forensic Readiness BYOD Implementation. We have conducted a two-phase study and, during the first phase of the study, we have used Check Point SandBlast for threat hunting mechanism, threat emulation, and forensic investigation [45]. SandBlast is implemented on the Check Point management server. For the forensic investigation, we have also used a forensic module of Check Point to find the source of attack and logs of malicious activity. Clustering of multiple gateways was used to conduct crime analysis for large-scale deployment for correlated view [12].

During the second phase of the study, we have used Palo Alto Cortex which is an AI-based security platform for cyber defense mechanisms and Palo Alto Firewall for capturing BYOD threat traffic and analysis as well as Panorama for management and reporting.

4. Results

After implementation of the BYOD digital forensic infrastructure, we have captured and analyzed the results. The results have been also compared, and significant advancement of cyber defense mechanisms in BYOD forensic has been observed. The clustering approach implementation shows multiple incidents and malicious activities. The malicious activity was also captured using Wireshark logs, and it was analyzed [33]. The malware was created to test the malicious activity, a postincident forensic investigation was conducted, and the result was captured.

4.1. Detection of Critical Attack in BYOD and Forensic Analysis

4.1.1. Critical Attack View. Based on the analysis and detection of malicious activity conducted in a BYOD environment, Figure 5 represents the resultant forensic analysis of a critical attack. This was captured on the endpoint using Check Point SandBlast tool. The attack happened and was captured as Process ID 9232 was an attack in nature, and after entry of the malware, file was renamed and deleted in the BYOD environment.

The malicious activity was performed intentionally, the result was captured, and it was observed that Trojan which tried to damage the system in the BYOD environment was detected. It tried to damage the critical infrastructure.

4.1.2. Critical Attack View from Forensic Analysis View of Cortex. Similarly, from Palo Alto Cortex, attack information was captured and analyzed. After attack in the BYOD infrastructure, the investigation was conducted to complete the analysis as per Figure 6.

The result from Cortex is clearly reflected in Figure 6.

4.1.3. Critical Attack Logs from Cortex. During the investigation, critical attack information was further analyzed with raw logs to track the source of the attack. Source IP address and destination are presented in Table 8.

The attack was from IP addresses 172.28.15.14, 172.28.3.220, and 172.28.1.164, which were used in the BYOD devices as internal IP addresses. During the investigation process, we clearly detected the user and malicious activities performed by the users. Sensitive and robust analysis was done so that manual conventional result can be compared with the simulated analytical result as to how analysis is done in a study of pressure relief [46].

Table 6: Index used in Figure 4.

Index	Description
22	Palo Alto 3020 as firewall for capturing BYOD traffic
23	PA event log management M-200
24	Palo Alto Cloud Cortex
25	The span of BYOD traffic going towards the Internet
26	Event log traffic towards Panorama

Table 7: DMZ firewall open ports for the testing.

Sl. no.	Firewall	Source	Destination	TCT/UDP port
1	DM firewall	Foreign controller	Anchor controller	EoIP tunnel port
2	DMZ firewall	Foreign controller	ISE	1812
3	DMZ firewall	BYOD user	DNS	53
4	DMZ firewall	BYOD user	ISE	8443
5	DMZ firewall	BYOD	AAA server	8907

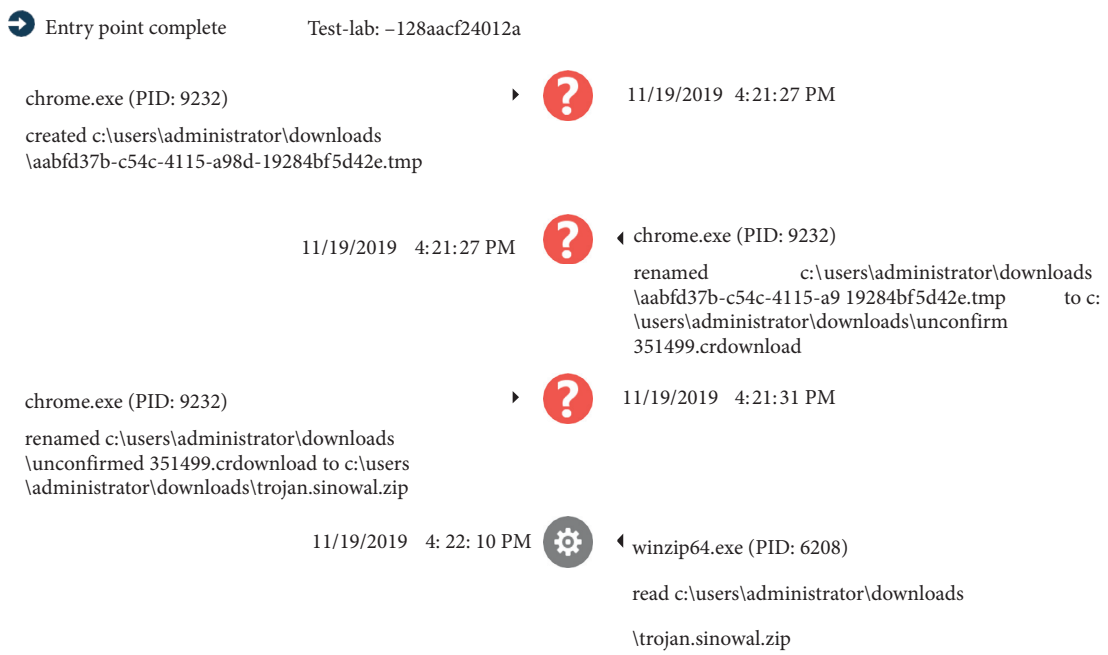


Figure 5: Critical attacks in the BYOD environment captured.

This traffic was captured from the architecture of Figure 4 and index 23. The malicious traffic observed in Cortex and cyber defense system was built to prevent those attacks as well, which is shown in Table 5.

4.1.4. Forensic Analysis from BYOD Endpoint. After analysis of malicious activities from gateway level, the next level investigation was conducted from the endpoint after identifying the attack source from sandblasting. Threat emulation shows the absolute result of malicious activities by endpoint BYOD devices as illustrated in Figure 7.

The result shows that malicious activity was detected during the preauthentication of the BYOD users, with a preauthentication segment IP address (192.168.1.x). One of the phishing attack packets was captured after an attack, and the details of the attack are represented in Figure 8(a).

This packet has the source IP address 172.28.1.164, attack type was phishing attack, and also user identity was traced from the Cisco Identity Service Engine during the test as per Figure 3, index 9. User identity was identified after the attack. This result was captured after detection of the endpoint performing reverse analysis from SandBlast from gateway level. Logs were captured for forensic analysis case event type from BYOD gateway as per Table 9.

The logs of this attack were captured after an incident, and we conducted the analysis of the threat. The attack ID is a4640108-ce8b-af06-5dd7-9aa500050000. Traffic from 172.28.1.164 was an attack, and traffic was decrypted in the gateway level. Besides, as seen in the result, the system was "Windows 10.0 Enterprise Edition" and the "Gen.SB.exe" was detected in the system which accessed c:\\users\\imanali\\desktop\\340s.exe. Finally, Trojan was detected.

The mentioned threat landscape detail was captured.

Table 8: Attack traffic captured from index 23, Figure 4.

Alert Id	Timestamp	Host	Host IP	User name	Severity	Alert
Source	Action	Category	Alert Name		Description	
	Initiated By		Initiator CMD		Initiator	
signature	Initiator signer		Event Type		CGO name	
	CGO CMD		CGO signature		CGO signer	
	CID	Target process name		Target process CMD		
	Process execution signature			Process execution signer		
	Target process SHA256			File path	File MD5	File
SHA256	Registry data		Registry full key		Local IP	
	Local port	Remote IP	Remote port		Remote Host	
	App -ID	Excluded	Starred	External Id		
32	Dec 21st 2019 10:30:20			172.28.15.14		
	172.28.15.14			High	PAN NGFW	
	Detected (Raised An Alert)			Spyware Detected via Anti-		
Spyware profile	Threat ID #109000001			None		
(S u spicious DNS Query (vltwox7zl7h1wv.com))						
	N/A	N/A	Netw ork Event			
	N/A	N/A				N/A
	N/A					
		172.28.15.14		39830	4.2.2.2	53
	dns	False		False	4662551	
14	Dec 18th 2019 14:25:15			INDELTEST		
	172.28.1.164		imanali	High	XDR Agent	
	Prevented (Blocked)		Malware	Behavioral Threat		
	Behavioral threat detected			mcpatcher.exe		
	"""C:\Users\imanali\Downloads\mcpatcher.exe"" "					
	N/A	Solimba Aplicaciones S.L.			Process	
Execution			N/A	N/A		
		N/A	N/A			
				False	False	
	1c1392bc217411eab7a1507b9d62f9c8					
12	Dec 18th 2019 14:25:08			INDELTEST		
	172.28.1.164		imanali	High	XDR Agent	
	Prevented (Bloc ked)		Malware	Behavioral Threat		
	Behavioral threat detected			mcpatcher.exe		
	"""C: \Users \imanali \Downloads \mcpatcher.exe"" "					N/A
	Solimba Aplicaciones S.L.			Process Execution		
		N/A	N/A			
	N/A	N/A				
			False	False		
	1789333c217411ea8e44507b9d62f9c8					
9	Dec 18th 2019 14:18:39			INDELTEST		
	172.28.1.164		imanali	High	XDR Agent	
	Prevented (Blocked)		Malware	Behavioral Threat		
	Behavioral threat detected			mcpatcher.exe		
	"""C: \Users \imanali \Downloads \mcpatcher.exe"" "					N/A
	Solimba Aplicaciones S.L.			Process Execution		
		N/A	N/A			
	N/A	N/A				
			False	False		
	3007c51e217311ea9fad507b9d62f9c8					
1	Dec 18th 2019 12:46:58			172.28.3.220		
	172.28.3.220			High	PAN NGFW	
	Detected (Raised An Alert)			Spyware Detected via Anti-		
Spyware profile	Threat ID #109000001			None		
(Suspicious DNS Query (7cfr5a9yjm3p.n9aupi94u3yt.com))						
		N/A	N/A	Network Event		
		N/A	N/A			
	N/A	N/A				
			172.28.3.220		58380	
	4.2.2.2	53		dns	False	False
	3401539					

This was an artifact after BYOD threat analysis with different risk, attack, and forensic information.

4.1.5. BYOD Environment Cyberattack Category Analysis. During the research, the different types of attacks in BYOD environment were reviewed and categorized by risk and criticality. The attack categorization framework was analyzed. Different attack event was framed.

We have captured a total of 966 packets from Check Point for analysis with different risk severity. Based on risk, the categorization of the traffic analysis result is shown in Figure 9.

The attack categorization framework was captured as per MITRE ATT&CK as shown in Figure 10.

5. Comparison and Analysis of Existing Technology

After conducting the research comparison and analysis, our prime focus was to find out the uniqueness of this simulation. Results and outcomes were compared with the existing available model of the threat detection process. While existing methods and techniques are quite effective in detecting known threats and protecting known threats, DNS layer security mechanism is not enough to protect. As per Cisco research, 91% of the malware attacks are in DNS layer [47] while the majority of the organizations do not have a mechanism for detection and protection. For unknown threat portfolio, available solutions of sandboxing are effective, but since the threat landscape is increasing day by day with new behavior, even an effective solution is not mitigating the new advanced threats. For better understanding, a graphical representation is used in Figure 11 for available solutions and limitations.

Figure 12 shows the limitations to the mitigation of a new zero-day malware attack.

An attack that is brand new or zero-day cannot be detected, and this might disrupt the business system such as the attack shown in the simulation.

In order to mitigate this situation, an advanced level of detection and protection mechanism is an upcoming requirement.

This research has a potential mechanism to detect attacks targeting system memory or CPU level attacks. As shown in Table 8, a system-level attack which executes commands at the process level was observed.

Dec 18th 2019 14:25 :08		INDELTEST		172.28.1.164
	imanali	High	XDR Agent	Prevented
(Blocked)	Malware	Behavioral Threat	Behavioral threat detected	
	mcpatcher.exe			
	"""C:\Users\imanali\Downloads\mcpatcher.exe"" "			N/A
	Solimba Aplicaciones S.L.	Process Execution		

This was a zero-day attack that has not been identified by AntiVirus, AntiBot, or IPS as this was a brand new malicious

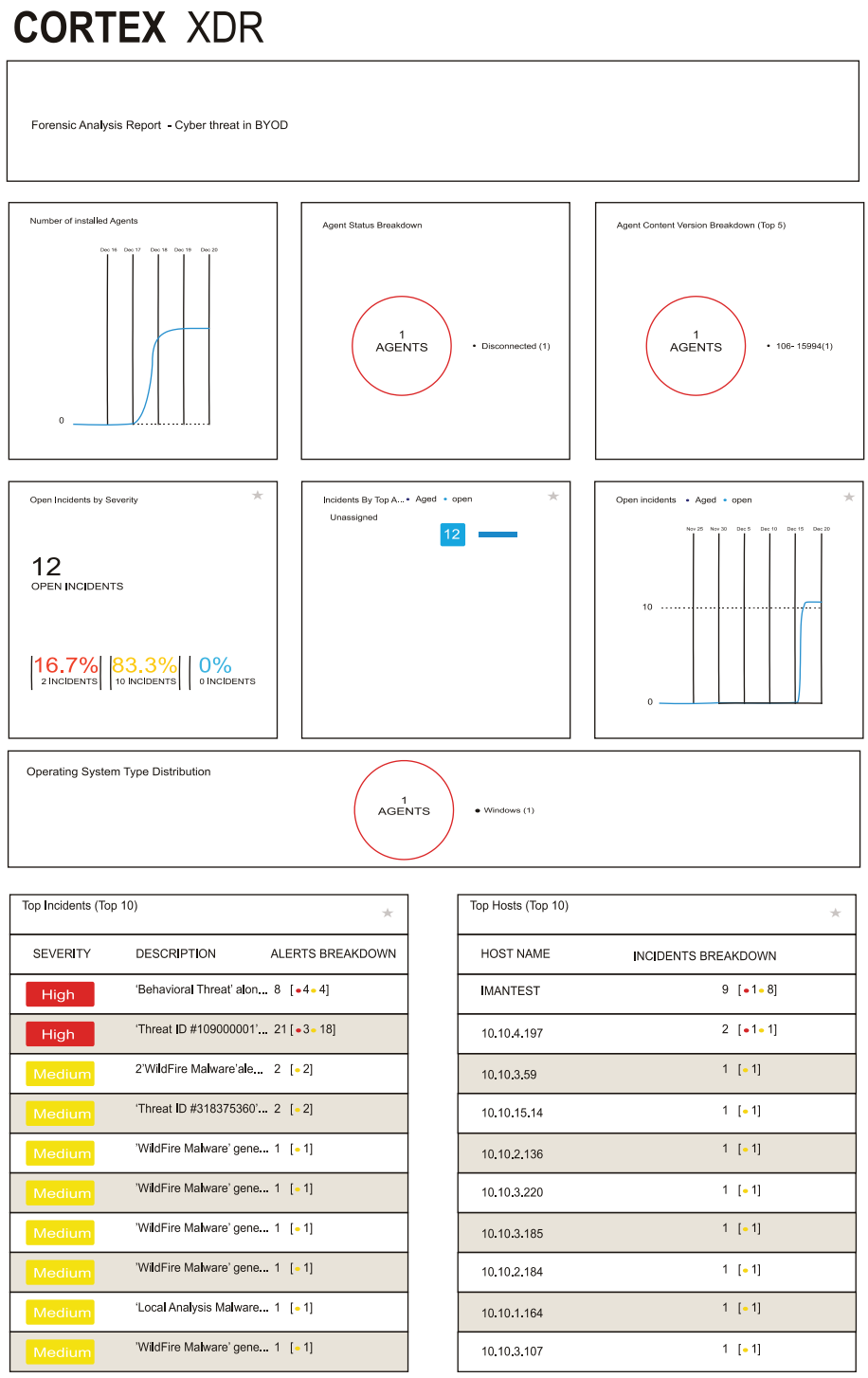


Figure 6: Malicious traffic captured from architecture of Figure 4, index 23 from Palo Alto as per design.

code that attacked the BYOD environment. Even regular sandboxing mechanism did not work to quarantine or to block it.

The architecture of the advanced threat detection model proposed in this research is shown in Figure 11.

The proposed model is shown in the sequential manner of events in Figure 11. In sequence 1, CPU starts processing, and hypervisor is running in 2 along with OS in sequence 3. After setup of the minimum requirement, application is accessed through any native application. Monitoring of CPU

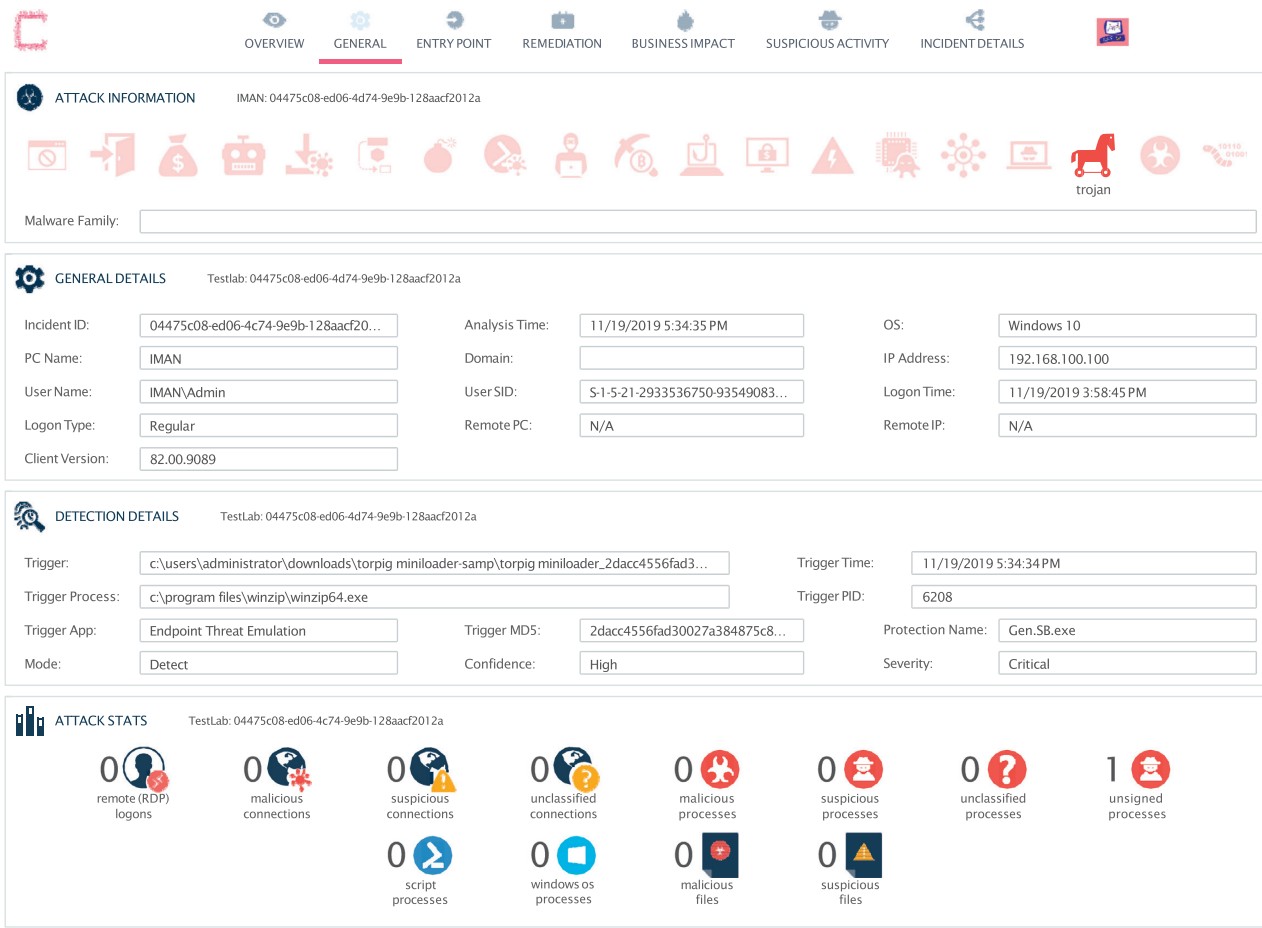


Figure 7: Malicious activity analysis from BYOD endpoint using SandBlast Agent (Figure 3, index 5), Check Point.

activities is in sequence 5 which is a key focused area in this process. If any malicious activities are observed in sequence 6, anomalies detection and protection mechanism is called in sequences 7 and 8. Sequence 9 protects the system before an attack so that BYOD environment cannot be exploited.

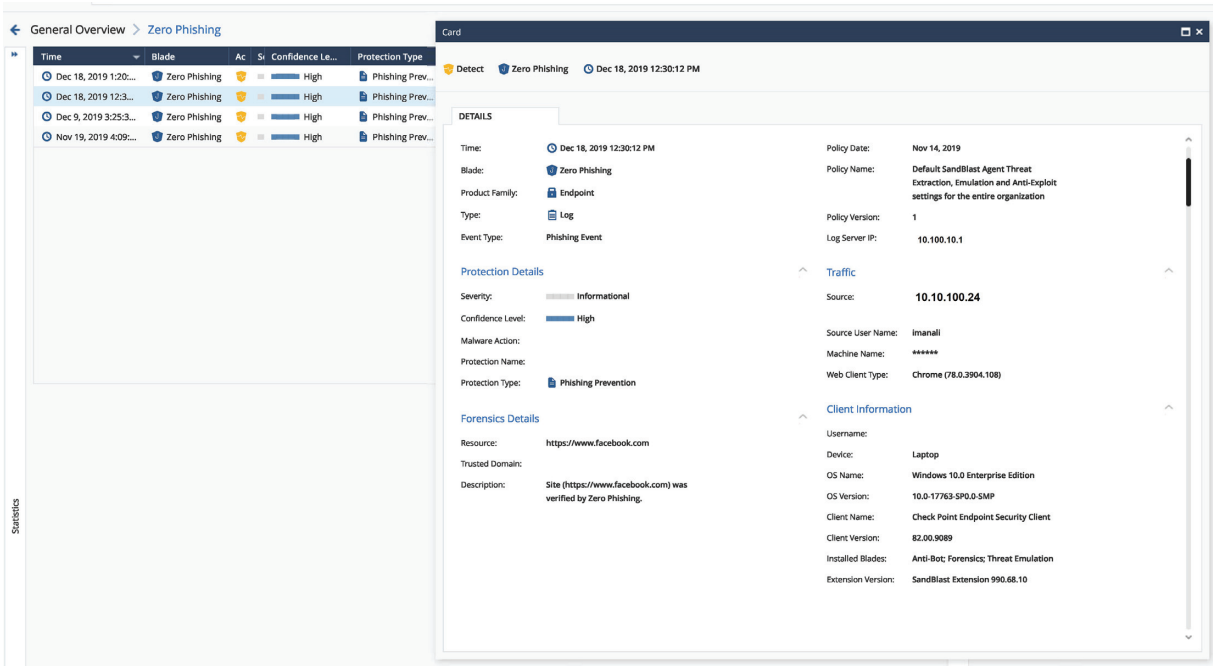
Comparison and benefit of the new technique are provided in Table 10.

The comparison of the existing mechanisms and the proposed mechanism is a comprehensive technique in protecting the organization before a potential attack by analyzing the behavior of the malicious activities from the CPU level in the BYOD environment.

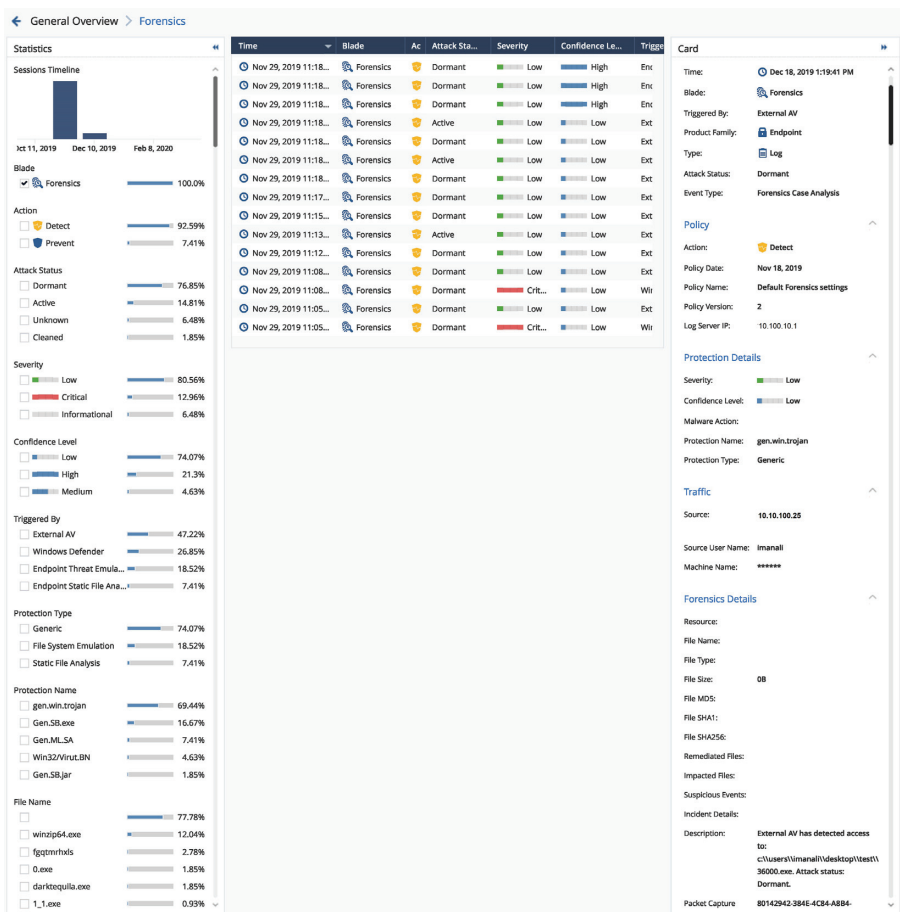
6. Proposed Cyber Forensic NG-DFR Model

After analysis of the results, an advanced level of the cyber forensic model concept is formalized. Next-generation digital forensic (NG-DFR) model is proposed to complete the process of investigation. This model is proposed with the major components as BYOD process definition, then BYOD technology enablement, threat hunting mechanism as the 3rd component, thereafter protection mechanism as the 4th component, and at last forensic process, law, and enforcement as the 5th component. All these 5 components of collaboration approaches in the cyber forensic environment are presented to build a cyber forensic ecosystem. The major 5 component modules described prove the concept of the next-generation DFR model.

6.1. BYOD Cyber Forensic Process Definition. The first and foremost task is the process layout of the BYOD environment. Framework for cyber secured BYOD policy is where untrusted devices are provisioned to access resources over critical infrastructure. In this phase, the security policy definition is framed. After policy of detection mechanism environment is framed, this can comprise multiple technologies and processes. In this phase, the attack detection mechanism is framed. After detection policy violations and acceptance policy are defined, the incident handling mechanism and security operation center mechanism are defined along with the integration of multiple products, and the technology framework is defined in this phase. At last,



(a)



(b)

Figure 8: (a) Phishing attack analysis packet captured. (b) The detailed cyber threat landscape in BYOD environment.

Table 9: Forensic case analysis after attack.

Nov 22, 2019 8:21:57 AM imanali Anti-Bot; Forensics; Threat Emulation Log 2019-11-22T08:35:47Z
Forensics Case Analysis 2019-11-22T13:51:57Z 2019-11-18T14:19:55Z Detect a4640108-ce8b-af06-5dd7-9aa500050000 1 Active 1 ep-demo 0 @A@@B@1574380800@C@52 Gen.SB.exe 46133eec-f86a-480f-a2dc-7483e2c20adf 1.57441E+12 High Endpoint Threat Emulation has detected access to:c:\\users\\imanali\\desktop\\340s.exe. Attack status: Active. Laptop INDELTEST 2 Endpoint Threat Emulation 82.00.9089 Check Point Endpoint Security Client 0 Critical Endpoint Forensics ip-172-28-1-164.ec2.internal (172.28.1.164) 10.0-17763-SP0.0-SMP Default Forensics settings File System Emulation 0 (10.128.140.176) 164.100.1.8 true S-1-5-21-2933536750-935490830-805106884-1003 Generic″, \″Trojan″, Windows 10.0 Enterprise Edition

the complete security posture framework is laid down in this phase as shown in Figure 2.

6.2. BYOD Technology Enablement. BYOD technology enablement is an important key area in this proposed concept of NG-DFR. Different products and technologies enabled the complete service. While choosing products and technology, the most important factor to consider is the integration of different products and technology. If advanced level networking and security products and technology are placed but all these do not talk with each other, then threat intelligence in NG-DFR will be a challenge. Accordingly, in this phase, major service enablement products and technology are factored to work in an integrated way so that each and every threat can be traced without any break of the packet flow. As shown in Figure 4, integration was done along with Cortex for the data lake. Apart from this in Figure 3, integration of next-generation endpoint protection is also introduced for the threat hunting process to enable critical infrastructure. In this section, actual threat detection technology is integrated with the authentication of BYOD users. After secure authentication and onboarding [43], detection of malicious traffic mechanism is proposed [48]. Log management and sandboxing for traffic analysis are considered in this phase.

6.3. Threat Hunting Framework. The most important key part for the forensic investigation ecosystem to develop is the threat hunting mechanism. Monitoring is a continuous action to collect activity logs for potential threat detection in a cyber forensic system. After an attack, finding the source of the attack is a critical task [8]. Detection of malicious [49] traffic which is indeed a major dependent technique required in cyber forensic mechanism is introduced in this phase. Primarily in this section, log analysis is conducted in order to track suspicious traffic. Once the threat is detected in this phase, threat verdict and score are checked to determine whether it is malicious or not. If it is found to be malicious and known pattern, then protection [48] module is called. If the threat pattern is unknown by the threat defender, for example, a zero-day attack [50], then, after extraction of hash, it is sent to threat cloud for verdict and score of the threat and retrospective event is triggered [51]. Finally, logs are preserved for further investigation. In this section, endpoint traffic logs are captured in the external gateway as shown in Figure 3 index 8 and Figure 4 index 23 so that later on logs can be investigated further. Apart from this, all traffic including source IP, destination IP, user information, and user MAC address is captured with all activity details.

6.4. Threat Protection Mechanism. Protection from threat is the foremost task before an attack on the organization. Consistently, researchers are focusing on developing new tactics for threat protection. Different types of novel approaches have been developed in threat protection. One of the advanced level protection mechanisms was developed in BYOD cyber forensic ecosystem study [48]. In this phase, concept of protection of critical infrastructure is covered. After getting the threat category, traffic dropped and logs are preserved for analysis as shown in Figure 3 index 13, and results are shown in Figure 8(b).

6.5. Forensic Investigation, Law, and Enforcement Module. In this phase, a forensic paradigm is presented. In order to complete the forensics of attack, few key areas need to be focused on such as analysis of the logs, preservation of the traffic, and stored log. After analysis, presentation and documentation need to be done. The entire BYOD ecosystem has to have the ability to do all these activities. Preserving evidence and log correlation is focused on the integration of different technologies and products as shown in Figures 3 and 4, where all the gateway perimeter security devices along with AAA, controller, and BYOD users are integrated with Active Directory user database. After integration, end-to-end logs analysis mechanism is developed to enable the forensic system. Finally, forensic correlation of related facts and finding is documented and presented.

7. Next-Generation DFR Model Ecosystem

In this phase, the final framework is represented by next-generation digital forensic readiness (NG-DFR) model. Step by step sequential process is explained to complete the cyber forensic ecosystem. The complete ecosystem comprises process, policies, humans, technology, and integration. Integration of process and technology with human interaction area is covered to build cyber forensic BYOD environment. As shown in Figure 13, complete steps are proposed for next-generation DFR model.

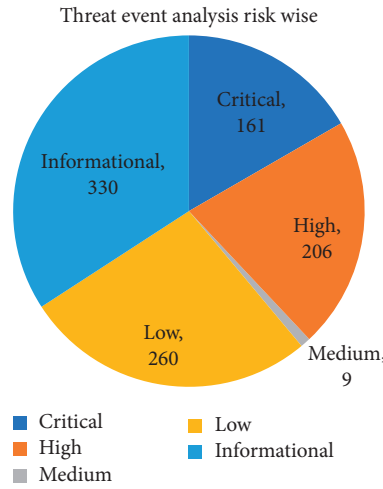


Figure 9: Risk-wise traffic analysis out of 966 packets.

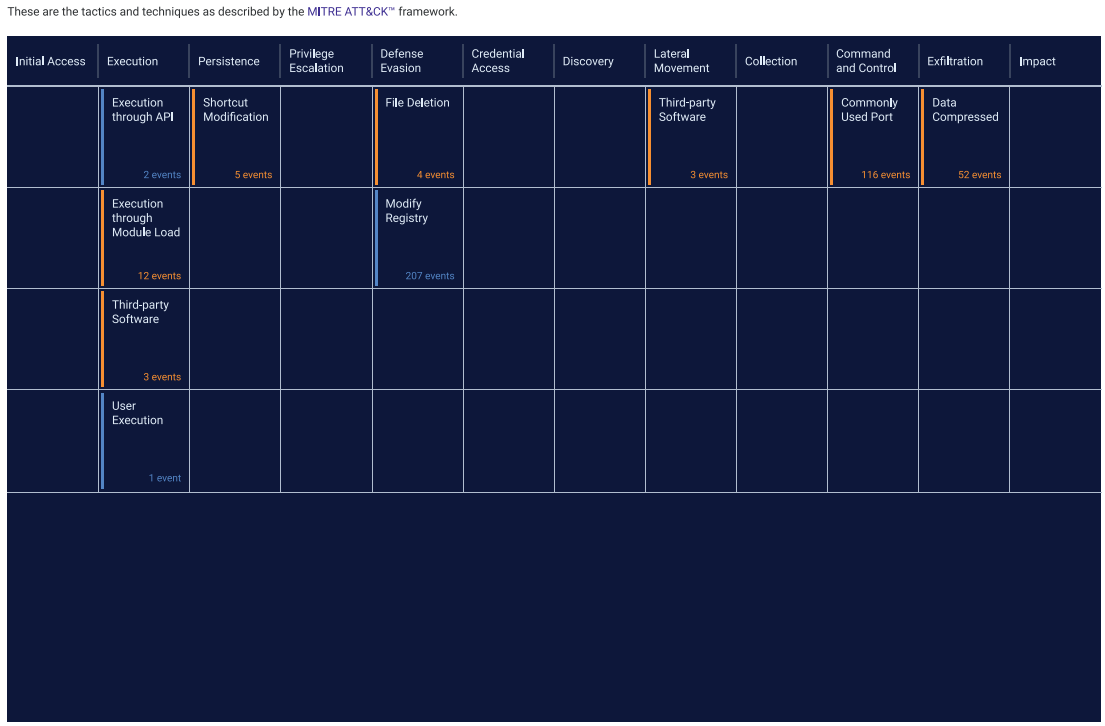


Figure 10: Attack framework as per MITRE ATT&CK.

In Step 1 of the NG-DFR model in Figure 13 planning, policy frameworks are defined with related security and technology enablement paradigm. Service enablement policy, security policy, and detection policies alert mechanism are defined. The integration process is defined.

In Step 2 Service enablement area is focused on. In particular, to build secured BYOD infrastructure with all required products and technology is a key component of this phase.

In Step 3 specially, a detection mechanism is proposed. Detection of various threats and then categorization of the threats are sequential events. Malicious traffic and known threats are detected, and unknown threats are filtered. Unknown threats are sent to the threat cloud in this phase to be analyzed and get the threat score so that appropriate action can be taken.

In Step 4, protection of critical infrastructure is focused on. Protection from different threats before exploiting up to best possible options is taken care of so that the threat landscape can be reduced.

In Steps 5 and 6, the focus area of NG-DFR that is a thorough investigation of the threat is covered. In this phase, outcome of the integration of all tools, techniques, products, and technology are leveraged to build a cyber forensic ecosystem. After analysis from preserved logs, threat hunting mechanism is enabled to carry out the investigation. Finally, storing the logs and artifacts and preparing documentation for submission to law and enforcement are covered.

In a nutshell, this proposed approach of NG-DFR model covered end-to-end system to complete the forensic

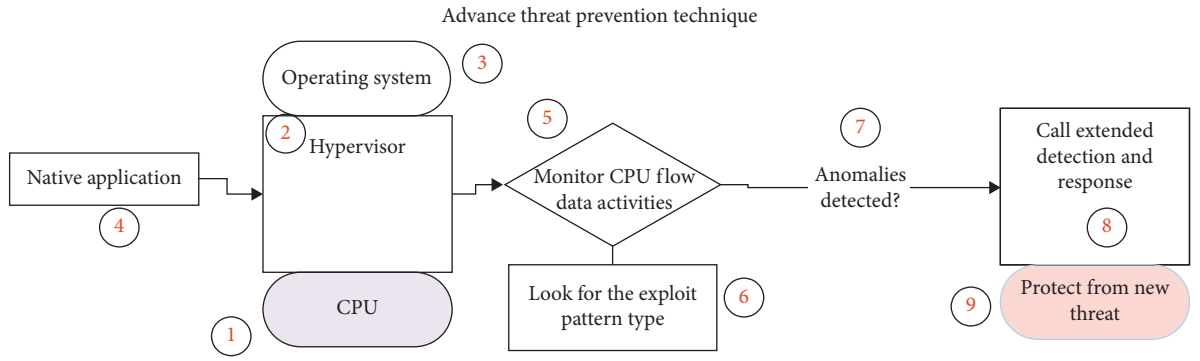


Figure 11: The proposed new approach of the threat detection model.

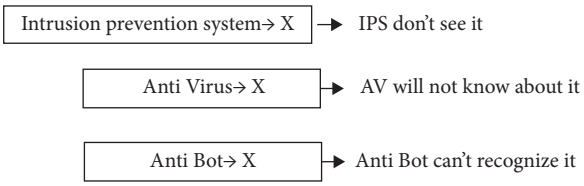


Figure 12: Existing technology to handle the attack.

Table 10: Comparison of the existing solutions and the new simulated solution.

Threat type	IPS (intrusion prevention system)	AntiBot	AntiVirus	New proposed model
Known threat	Yes	Yes	Yes	NA
Unknown threat detection	No, until sandboxing, and more time consuming	No, until sandboxing process which is more time consuming	No, protection mechanism time is higher	Yes, protecting before attack

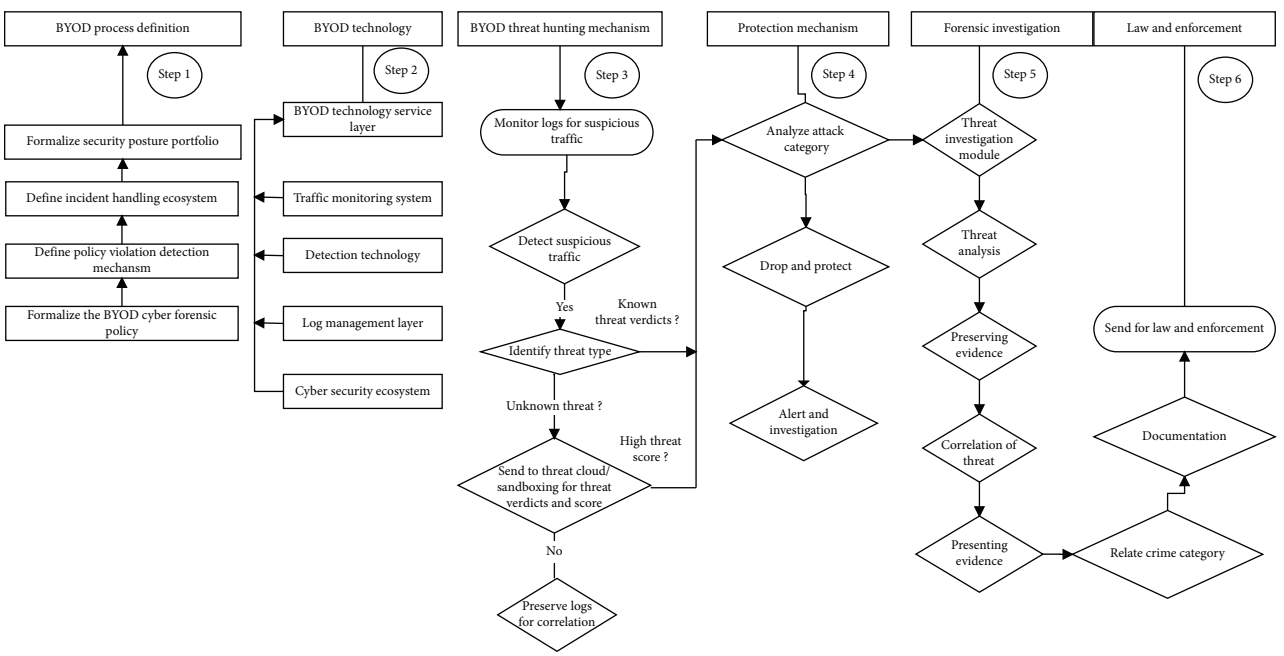


Figure 13: Next-generation digital forensic framework.

```
Step 1: Start
Step 2: Define BYOD security process and policies variables
   P1 = Security policies
   P2 = Detection Polices
   P3 = Incident Response
   P4 = Security violation Protection policy
   P5 = Forensic call policy
Step 3: Technology variables and users
   T1 = Technology portfolio
   T2 = Monitoring system
   T3 = Detection System/Decoy system
   T4 = Protection technology
   T5 = Log management
   T6 = Forensic technology ecosystem
   T7 = Threat category
   U1=BYOD users
Step 4: action and category variables
   violation = V
   Risk acceptable level = A
   Protection = P
   Forensic = F
Step 4: Monitoring of threat
   push U1 through T3 and compare P1
   If Result = A
      then accept request
      stop
   else
      call Step 5
   Then process U1 in T4 for P2
      send U1 logs to T5
   else
      call step 5
Step 5: Detection and Protection
   Push U1 through T3 for P4
      if Result = V
      Drop traffic
   Else
   call step 7
Step 7: identify threat
   If threat category is = known
      if verdict/score = A
         pass the traffic
      else
         drop and send Call step 10 for forensic
   else
         call step 8 for T7 Sandboxing for threat verdicts to
         call step 9
   else
      call step Sandboxing for threat verdicts
Step 8: Analyze threat category
         Analysis of threat type with threat Hash
         return T7 = verdict and score of threat category
Step 9: Unknown threat for forensic
         If T7 = = A compare to P5
            pass and send T5
         else
            send for forensic T6
Step 10: Forensic ecosystem
         if P5=Investigate attack
            do analysis
         Present
Step 9: Present to Law and enforcement
Step 11: Stop
```

Algorithm 1: Detailed algorithm of NG-DFR model.

investigation in order to build an advanced level of the cyber forensic ecosystem.

Detailed algorithm of NG-DFR based model is shown in Algorithm 1.

An algorithmic approach for NG-DFR model is proposed as per architectural flow shown in Figure 13.

8. Discussion

With BYOD, being external devices connected in the infrastructure, it is very sensitive and critical in nature to control threats and postincident analysis of the attack, and finding the source of the attack is a very crucial part. As per Check Point technology research, 99% of organizations [52] do not have a protection mechanism to fight against the ongoing cyber-attack threats. The proposed approach of NG-DFR has addressed the need for an end-to-end cyber forensic ecosystem.

After any cyber incident, finding digital evidence, analyzing the evidence, preserving and presenting the evidence for legal requirement for the court of law are important requirements. This research developed a new model of investigation of a different attack, reaching up to the endpoint of the attack which was targeted during the research. Network security, endpoint security, and critical infrastructure security all are covered in this research with respect to protection of critical infrastructure from BYOD threat.

During the investigation process in BYOD, after an attack, we analyzed all different categories of attack and behavioral analysis of crime. As it was also an important target to protect the infrastructure, detection and prevention were also achieved. Honeypot technology used for detection was not enough to protect the infrastructure. There was a need for prevention technologies after detection by the system without manual intervention. STRIDE-based threat model, which is an interaction between the threat and the corporate network, can be integrated with this model to get a better result.

End-to-end visibility, analysis, investigation, and integration between tools and technologies for building up an advanced model of cyber defense system were needed to fight against today's advanced cyber threat landscape. During the research, an advanced level of cyber forensic model was developed.

Moreover, one important aspect was analyzed during the research, which is run time detection of attack endpoint, status of connection and blocking, and preventing the endpoint from the infrastructure. Detection of threat, visibility of threat associated risk, incident response, and postincident forensic model are key areas explored in this research.

9. Contribution

There are two major novel contributions from this research. The first research contribution is a unique attack detection mechanism. This unique attack detection mechanism helps to detect and protect against zero-day attacks which cannot be detected by traditional tools like IPS, IDS, AV, and AntiBot. The second key contribution is to build a cyber defense BYOD ecosystem. This research has contributed to the area of cyber forensic analysis of a BYOD environment. The complexity of forensic analysis of the malicious activity in a BYOD environment is simplified. The different approaches of forensic investigation are compared using different tools and techniques. Finding the source of an attack in BYOD is analyzed from internal and external threats. The threat prevention mechanism is also an important contribution to this research, and end-to-end BYOD cyber forensic ecosystem framework is also defined.

10. Future Research

Digital forensic investigation becomes complex due to lack of standard procedures depending upon the types of digital crime. The growing complexity of crime becomes a challenge to face with standard tools and techniques. Since BYOD adoption is an upcoming growing phase, new tools and technologies are used by criminals to conduct crimes in zero-day attack behavior. Therefore, ongoing further research is important to fight against crimes. Also, an important area of further research is the collaboration of cyber tools, technology, and cyber law.

11. Conclusion

Due to the lack of a cyber defense ecosystem in the BYOD environment, attacks on the critical infrastructure of the organizations increased, and as a result business ecosystem gets fragmented. Cyber secured BYOD infrastructure is one of the major requirements for organizations today to protect from the advanced level of threats. In this paper, a framework of the cyber forensic model is presented including a cyber-secure BYOD model.

In the first phase of this research, the detection technique of threat is explored with different tools and techniques for further research and analysis.

In the second phase of this research, a major conclusion is a novel approach of detection and protection mechanism of zero-day attacks which cannot be detected by traditional tools like IPS, IDS, AntiBot, and AntiVirus. The proposed method of detection and protection model of unknown threats or zero-day attacks contributed to the protection of the organization's critical infrastructure. The comparison of the outcomes shows a significant advanced incremental positive result, and adoption of this method helped to build the complete cyber forensic ecosystem.

Postincident threat hunting is a critical task in any cyber forensic investigation which is addressed in this research using different tools and techniques like sandblasting and Cortex.

Finally, an advanced level of cyber forensic readiness BYOD infrastructure is developed. Next-generation digital forensic readiness (NG-DFR) model is proposed to mitigate the ongoing need for conducting end-to-end digital forensic investigation including detection and protection framework which also includes the BYOD policy framework and service enablement technology area.

Data Availability

The design/data/architecture used to support the findings of this study are included within the article.

Disclosure

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] H. Shetty, L. Unden-Farboud, and P. Arriandiaga, "Competitive landscape: managed mobility services," 2020.

[2] "94% enterprises will use IoT by end 2021: Microsoft report," 2019, https://www.livemint.com/technology/tech-news/94-enterprises-will-use-iot-by-end-2021-microsoft-report-15651654498 42.html.

[3] B. Tokuyoshi, "The security implications of BYOD," *Network Security*, vol. 2013, no. 4, 13 pages, 2013.

[4] J. Collie, "A strategic model for forensic readiness," *Athens Journal of Sciences*, vol. 5, no. 2, pp. 167–182, 2018.

[5] M. Ratchford, P. Wang, and R. O. Sbeit, "BYOD security risks and mitigations," in *Information Technology-New Generations*, S. Latifi, Ed., pp. 193–197, Springer International Publishing, Cham, Switzerland, 2018.

[6] "Risk or reward: What lurks within your IoT?," 2017.

[7] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Smart airport cybersecurity: threat mitigation and cyber resilience controls," *Sensors*, vol. 19, no. 1, p. 19, 2018.

[8] 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*, Á. Rocha, H. Adeli, L. P. Reis, and S. Costanzo, Eds., pp. 252–262, Springer International Publishing, Cham, Switzerland, 2019.

[9] P. Beckett, "BYOD-popular and problematic," *Network Security*, vol. 2014, no. 9, 9 pages, 2014.

[10] "Browse cve vulnerabilities by date." https://www.cvedetails.com/browse-by-date.php, 2019).

[11] 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, 2019.

[12] V. R. Kebande, N. M. Karie, and H. S. Venter, "A generic Digital Forensic Readiness model for BYOD using honeypot technology," in *Proceedings of the 2016 IST-Africa Week Conference*, pp. 1–12, Durban, South Africa, May 2016.

[13] "Union Home Minister inaugurates Cyber Crime Unit of Delhi Police and National Cyber Forensic Lab." 2019, http://pib.nic.in/newsite/PrintRelease.aspx?relid=188700.

[14] Vishnu Institute of Technology, B. V. P. santhi, P. Kanakam, and S. M. Hussain, "Cyber forensic science to diagnose digital crimes-a study," *International Journal of Computer Trends and Technology*, vol. 50, no. 2, pp. 107–113, 2017.

[15] Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia, Y. Prayudi, A. Ashari, and T. K. Priyambodo, "A proposed digital forensics business model to support cybercrime investigation in Indonesia," *International Journal of Computer Network and Information Security*, vol. 7, no. 11, pp. 1–8, 2015.

[16] S. Soltani and S. A. H. Seno, "A formal model for event reconstruction in digital forensic investigation," *Digital Investigation*, vol. 30, pp. 148–160, 2019.

[17] S. Ghosh, P. Shivakumara, P. Roy, U. Pal, and T. Lu, "Graphology based handwritten character analysis for human behaviour identification," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 55–65, 2020.

[18] L. Columbus, "83% of enterprise workloads will Be in the cloud by 2020," 2020, https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/.

[19] D. Kim and S. Lee, "Study of identifying and managing the potential evidence for effective android forensics," *Forensic Science International: Digital Investigation*, vol. 33, Article ID 200897, 2020.

[20] S. L. Garfinkel, "Digital forensics research: the next 10 years," *Digital Investigation*, vol. 7, pp. S64–S73, 2010.

[21] C. Utter, "The "Bring your own device" conundrum for organizations and investigators: an examination of the policy and legal concerns in light of investigatory challenges," *Journal of Digital Forensics, Security and Law*, vol. 10, no. 2, 2015.

[22] "Digital Forensics in the Mobile, BYOD, and Cloud Era,".

[23] S. J. Ngobeni, "Digital forensic readiness for wireless local area networks," 2016.

[24] A. Marotta and M. McShane, "Integrating a proactive technique into a holistic cyber risk management approach," *Risk Management and Insurance Review*, vol. 21, no. 3, pp. 435–452, 2018.

[25] 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*, vol. 7, 2018.

[26] M. Kaur, D. Singh, V. Kumar, and K. Sun, "Color image dehazing using gradient channel prior and guided L0 filter," *Information Sciences*, vol. 521, pp. 326–342, 2020.

[27] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5 D chaotic map," *Future Generation Computer Systems*, vol. 107, pp. 333–350, 2020.

[28] S. Brotsis et al., "Blockchain solutions for forensic evidence preservation in IoT environments," 2019, http://arxiv.org/abs/1903.10770.

[29] D. A. Flores, F. Qazi, and A. Jhumka, "Bring your own disclosure: analysing BYOD threats to corporate information," in *Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA*, pp. 1008–1015, Tianjin, China, August 2016.

[30] I. Ali and S. Kaur, "Detection and control of malicious activity and digital forensic in BYOD," 2019.

[31] Z. A. Baig, P. Szewczyk, C. Valli et al., "Future challenges for smart cities: cyber-security and digital forensics," *Digital Investigation*, vol. 22, pp. 3–13, 2017.

[32] F. Servida and E. Casey, "IoT forensic challenges and opportunities for digital traces," *Digital Investigation*, vol. 28, pp. S22–S29, 2019.

[33] "Wireshark Go Deep." https://www.wireshark.org/, 2019.

[34] X. Zhang and K.-K. R. Choo, "Digital forensic education an experiential learning approach," 2020.

[35] S. Sathwara, N. Dutta, and E. Pricop, "IoT Forensic A digital investigation framework for IoT systems," in *Proceedigns of the 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pp. 1–4, Iasi, Romania, Jun. 2018.

[36] E. Casey, "The chequered past and risky future of digital forensics," *Australian Journal of Forensic Sciences*, vol. 51, no. 6, pp. 649–664, 2019.
[37] A. Gupta, D. Singh, and M. Kaur, "An efficient image encryption using non-dominated sorting genetic algorithm-III based 4-D chaotic maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1309–1324, 2020.
[38] "IBM Study: Responding to Cybersecurity Incidents Still a Major Challenge for Businesses - Mar 14, 2018," IBM News Room, 2019. https://newsroom.ibm.com/2018-03-14-IBM-Study-Responding-to-Cybersecurity-Incidents-Still-a-Major-Challenge-for-Businesses.
[39] "General Data Protection Regulation (GDPR) guidance," NHS Digital. 2019, https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance.
[40] "2017 Norton Cyber Security Insights Report-Global Results," 2018.
[41] B. Cusack and T. Laurenson, "Systems architecture for the acquisition and preservation of wireless network traffic," 2020.
[42] T. Wiens, "Engine speed reduction for hydraulic machinery using predictive algorithms," 2021.
[43] "BYOD secured solution framework," *International Journal of Engineering and Advanced Technology*, vol. 8, no. 6, pp. 1602–1606, 2019.
[44] "Group Encrypted Transport VPN (Get VPN) Design and Implementation Guide.
[45] D. Ghimire, E. Valle, and S. Robin, "Check point software technologies check point SandBlast agent next generation AV E80.82," 2020.
[46] S. Osterland and J. Weber, "Analytical analysis of single-stage pressure relief valves," *International Journal of Hydromechatronics*, vol. 2, no. 1, p. 32, 2019.
[47] "Cisco Security Report: Majority of Orgs Do Not Monitor DNS," Cisco Umbrella, 2016. https://umbrella.cisco.com/blog/cisco-security-report-more-orgs-should-be-monitoring-dns.
[48] I. Ali, "Byod cyber forensic eco-system," *International Journal of Advanced Research in Engineering and Technology*, vol. 11, no. 9, 2020.
[49] M. I. Ali, S. Kaur, A. Khamparia et al., "Security challenges and cyber forensic ecosystem in IOT driven BYOD environment," *IEEE Access*, vol. 8, pp. 172770–172782, 2020.
[50] A. Lamba, S. Singh, and B. Singh, "Mitigating zero-day attacks in IoT using a strategic framework," *SSRN Electronic Journal*, vol. 4, no. 1, 2016.
[51] Firepower Management Center Configuration Guide, Version 6.0 - File/Malware Events and Network File Trajectory [Cisco Firepower Management Center]," *Cisco*, 2020, https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01110001.html.
[52] Security CheckUp, Check Point Software." 2020, https://pages.checkpoint.com/security-checkup.html.