THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics,
Security and Law

Volume 16

Article 2

September 2021

DIGITAL FORENSIC READINESS FRAMEWORK BASED ON HONEYPOT AND HONEYNET FOR BYOD

AUDREY ASANTE
Catholic University College of Ghana, aud83uk@yahoo.co.uk

Vincent Amankona
Catholic University of Ghana, vincent.amankona@cug.edu.gh

Recommended Citation

ASANTE, AUDREY and Amankona, Vincent (2021) "DIGITAL FORENSIC READINESS FRAMEWORK BASED ON HONEYPOT AND HONEYNET FOR BYOD," *Journal of Digital Forensics, Security and Law*: Vol. 16 , Article 2.
Available at: https://commons.erau.edu/jdfsl/vol16/iss2/2

DIGITAL FORENSIC READINESS FRAMEWORK BASED ON HONEYPOT TECHNOLOGY FOR BYOD

Audrey Asante, Vincent Amankona
Catholic University of Ghana
aud83uk@yahoo.co.uk
vincent.amankona@cug.edu.gh

ABSTRACT

The utilization of the internet within organizations has surged over the past decade. Though, it has numerous benefits, the internet also comes with its own challenges such as intrusions and threats. Bring Your Own Device (BYOD) as a growing trend among organizations allow employees to connect their portable devices such as smart phones, tablets, laptops, to the organization's network to perform organizational duties. It has gained popularity over the years because of its flexibility and cost effectiveness. This adoption of BYOD has exposed organizations to security risks and demands proactive measures to mitigate such incidents. In this study, we propose a Digital Forensic Readiness (DFR) framework for BYOD using honeypot technology. The framework consists of the following components: BYOD devices, Management, People, Technology and DFR. It is designed to comply with ISO/IEC 27043, detect security incidents/threats and collect potential digital evidence using low- and high-level interaction honeypots. Besides, the framework proffers adequate security support to the organization through space isolation, device management, crypto operations, and policies database. This framework would ensure and improve information security as well as securely preserve digital evidence. Embedding DFR into BYOD will improve security and enable an organization to stay abreast when handling a security incident.

Keywords: cyber forensics, cyber security, digital forensics readiness, BYOD, honeypot technology

1. INTRODUCTION

The reliance on the internet has brought about a significant increase in crimes. Intrusions and attacks have been on the rise causing problems for organizations around the world (Velasco Silva Rodríguez Rafael, 2017). Every organization wants to ensure the safety of information and systems from attackers while connected to the internet. Intrusion attacks can be made by users (advance and novice actors), malware, bots etc. Most of these attacks have created challenges in identifying techniques and tools adopted in committing these crimes. Some attackers develop their own tools for these attacks, while others use already created tools. The ability to understand these attacks are based on the attacker's techniques and tools (Spitzner, 2002; Velasco Silva Rodríguez Rafael, 2017).

Pawlick et al., 2020 referred to techniques used by attackers to gain access to a network and elevate themselves to their targets. Many have proposed several methods in detecting and preventing attacks. Further studies (Cabaj, 2015; Chamotra et al., 2016; Gonzalez et al., 2020; Gudo Padayachee, 2015; Martin et al., 2017; Spitzner, 2002; X. Wang et al., 2019) have been done in identifying how to countermeasure attacks, but the dynamism of attackers' approaches have proven difficulties securing corporate systems. One security threat posing challenges is the Advanced Persistent Threat (APT). APTs are organized attacks not limited to state-sponsored activities, but to long-term hacking operations using advanced strategies, techniques and procedures by well-resourced adversaries against specific targets (Ahmad et al., 2019). They are the most advanced and strong class of security threat that causes security professionals problems because as an operation, it is goal oriented. According to (Pawlick et al., 2020), traditional security techniques are inadequate against APTs. Another important feature is to understand the attacker's motive which is to target devices that are easy to break through as compared to devices having vital information (Velasco Silva Rodríguez Rafael, 2017).

The introduction of Bring Your Own Device (BYOD) into organizations has exposed organizations to security risks. BYOD as a growing trend among organizations allow employees to connect their portable devices such as smartphones, tablets, laptops, to the organization's network. Employees use these devices to conduct their personal and official (business) duties, making them obviously cost-effective for organizations. Even though BYOD is cost effective for organizations, its security risks has also posed challenges for organizations. (Gudo Padayachee, 2015) and (Vignesh Asha, 2015) identifies security risks BYOD introduces into an organization. Some common threats to be encountered during BYOD adoption has been identified in (Simmons Vandeven, 2017). One main security challenge is employee privacy protection. (Gudo Padayachee, 2015) identifies end-user anonymity and leakage of private information as the two ways an employee's privacy can be breached.

Although intrusion and attacks on systems have increased, the introduction of honeypots and honeynets has been shown to help prevent and protect real systems as a countermeasure to attackers' intrusion. This countermeasure shows new attack mechanisms and intrusions by attackers if real systems are attacked. Honeypots can detect possible attacks in real time through log activity files and alerts. Honeypot is one of the most common tools for detecting malicious actions by using the masking technique (Gonzalez et al., 2020). Honeynets and honeypots are popular security mechanisms in capturing and analysing malware attack information. Honeypot is considered a system used to monitor passively. Honeynets are deception mechanisms which can benefit businesses when adopted. It also helps to design countermeasure strategies to safeguard networks for organizations. To prevent future attacks on the network of an organization, honeypots and honeynets can help IT professionals to be aware of new techniques, exploits and tools.

Digital Forensics has shaped how computer crimes are investigated and how criminals are prosecuted. As security incidents are bound to occur, organizations and individuals can rely on digital forensics to investigate and solve them. In the event of a security incident, an investigation must be conducted to determine the extent of the damage caused, the techniques used and the perpetrator. Digital forensic includes digital evidence recovery and analysis to identify events leading to a specific security incident (A. Kyaw et al., 2019; Sachowski, 2016). To make informed and appropriate decisions about business risks, organizations can incorporate Digital Forensic Readiness (DFR) to ensure the collection of data in an incident to guide investigators and stakeholders. DFR seeks to emphasize the expectation that an incident can occur thereby enabling organizations to efficiently gather data and rely on digital evidence instead of traditional response methods such as imaging of hard drives or devices (Rowlingson Ph, 2004). Digital evidence gathered during an investigation can serve as a means for proving, reducing, and supporting the impact of an incident. It can also serve to support legal processes and litigation issues. Organizations can rely on digital evidence to demonstrate compliance. DFR reduces the cost involved during a digital forensic investigation (Rowlingson Ph, 2004).

The aim of this paper is to propose a framework for BYOD to collect digital evidence from devices to protect and investigate data breaches. To ensure and improve information security in a BYOD environment, it is important for organizations to incorporate DFR. The proposed model is to meet the objectives of DFR.

2. BACKGROUND

This section reviews related works on BYOD, Digital Forensic Readiness, Honeypot and Honeynet.

2.1 BRING YOUR OWN DEVICE (BYOD)

BYOD is the use of employees' owned devices for official work. The reason for the growth of BYOD as a new trend is its cost effectiveness, familiarity and comfortability of employees using their own devices as compared to company devices. The use of personal devices enables employees to manage corporate activities from different locations. Advantages derived from BYOD includes the reduction in cost, mobility, flexibility, and the increase in employee's productivity. Apart from the advantages derived from BYOD, organizations need to understand the risks and liabilities that BYOD introduces when adopted. The adoption of BYOD as a strategy trend and addressing the challenges it poses is a predominant topic in the world today. The usage of smart devices allows the accessing of sensitive data during official use. This therefore requires the security of these devices to prevent attacks or unauthorized access of sensitive data. BYOD can cause organizations to face litigation problems unless appropriate security measures are put in place, including the protection of employees' privacy. Therefore, an acceptance of BYOD in an organization calls for a thorough security approach to employee actions and behaviours towards the usage of their own devices (Ratchford Wang, 2019). Eliminating the challenges in BYOD involves the study of techniques and methods of technical threats which can be used to access sensitive data. (Downer Bhattacharya, 2015) in their study identified the need for improving security in BYOD environments since the current frameworks are limited. Network Access Control challenges identified in their study can be improved or enhanced using honeypots. No emphasis was made on potential security solutions which could alleviate the current problems in BYOD security.

2.2 HONEYPOT

Identification and understanding of new techniques, tools and exploits is a challenge for network and security professionals. Honeypots are used to protect real systems through the monitoring of activities while being probed, attacked, engaged, or compromised. Honeypot is defined as a decoy system which attracts attackers to gather information about their actions (Pickett, 2003). As a monitoring system, it is used to identify potential attacks, threats, vulnerabilities, techniques, and tools.

Honeypots can be categorized into low-interaction, medium-interaction, and high-interaction (Pickett, 2003; Spitzner, 2002; Velasco Silva Rodríguez Rafael, 2017). Low-interaction honeypots are simulated systems that limits activities to be performed. It does not allow the capturing or identification of new exploits such as zero-day attacks. Another challenge is its ability to be detected easily by advanced or skilled attackers. High-interaction honeypots provide enough services for attackers to exploit compared to low-interaction honeypots. They are not emulated systems like low-interaction honeypots. The challenge is that these systems can be used to exploit other systems in the network. Medium-interaction honeypots rather provide more services than low-interaction but lesser services than high-interaction systems. It is therefore important to know how honeypots are implemented to enable the identification of potential attacks and threats (Cabaj, 2015). Honeypots can also be used for research or production (Pickett, 2003). A research honeypot is a high-interaction honeypot used to gather attacking information to discover new tools, techniques, activities, and motives during an attack. This type of honeypot can be used to caution and forecast future attacks and exploits, while production honeypot is a low-interaction honeypot used to detect and prevent attacks, as well as to provide response during an attack on an organization's systems. Honeypots can further be differentiated into virtual and real honeypots (Dalamagkas et al., 2019). Real honeypots have a better capability to attract and trap attackers as compared to virtual honeypots, but they are expensive.

2.3 HONEYNET

A honeynet is made up of high-interaction honeypots in a network to create security. Honeynets are valuable because of the ability to disguise. Several benefits can be derived during the implementation of honeynet, including knowledge of behavioural attack patterns, tools used, and strategies adopted by attackers. The data obtained by the honeynet can be analysed to establish techniques to avoid further attacks. A honeynet "emulates a set of sensors and controllers and records attacker activities" (Pawlick et al., 2020). Over the years, Honeynet has been introduced as a network security measure to collect attack information and detect malware, botnets, spam, and security breaches. As aiding tools, honeynets are known to be used to acquire intrusion signatures adopted in intrusion detection systems. Even though, attackers can detect current honeynet technologies, it is worth implementing them in an organization when much emphasis is placed on the disguise capacity during implementation. To prevent honeynets from being used as tools for security breaches, it is necessary to establish a highly controlled environment. A highly controlled environment is determined through the implementation of three requirements: Data Control, Data Capture and Data Collection (Pickett, 2003).

Honeynet Architectures Ist Generation or GenI honeynets are the simplest type of honeynet architectures (Pickett, 2003). Their purpose is to capture an attacker's activities. Data Control in GenI is designed to reduce risk and contain outbound operation of compromised honeypots so as not to harm non-honeypot systems. This is implemented using a dedicated network specifically for the honeynet and a routing firewall as access control device (Spitzner, 2002). In this type of honeynet, attackers are not allowed more freedom because outbound connections by the firewall can be limited. To greatly reduce risk, none or few outbound connections can be allowed by the firewall. To achieve Data capturing, logs and keystrokes are used.

Even though, it can capture more information and unknown attacks, it is ineffective in capturing advance attackers' exploits. GenI has the inability to detect encrypted attacks. In 2nd Generation or GenII honeynets, attackers are given the flexibility to explore. This architecture is used to capture and analyse threats. By using a difficult to detect IDS or layer-2 gateway, all inbound and outbound traffic must pass through this gateway (Spitzner, 2002). This type of honeynet can block or change outbound attacks. It also has the capability to increase deception by faking responses. GenII has been improved to detect encrypted attacks. GenII honeynets are effective in capturing advance attackers' exploits. 3rd Generation or GenIII uses honeywall which operates on the data link layer to capture and analyse attacks and exploits. It supports the correlation of obtained data (Velasco Silva Rodríguez Rafael, 2017). The honeywall has security tools such as Snort, Snort_inline, Argus, P0f, TcpDump, Sebek ,HFlowd, pcap, api and Walleye (Agnaou et al., 2018; Velasco Silva Rodríguez Rafael, 2017). It is easy to use and maintain because of the incorporation of data analysis into the same honeywall device (Velasco Silva Rodríguez Rafael, 2017). The honeywall has the capability to deceive attackers and its filtering device can be invisible during attacks. Except for the changes in GenII, GenII and GenIII are identical. Several studies have been carried out using honeypots and honeynets to detect, monitor, assess and report attacks and exploits. Honeypots and Honeynets have been used to conduct research in trending areas such as IOT, Cloud and Smart Grids. (Martin et al., 2017) adopted off-the-shelf low-interaction virtual honeypot daemon in their system for capturing signature attack patterns. These patterns were used to filter and stop potential traffic. The proposed system, Pot2DPI, is used to defend against IOT attacks. (Chamotra et al., 2016) created a system to detect bots and track botnets using honeynet. Their proposed system uses a distributed network of honeynet systems (low and high-interaction honeypots) to capture malware. (Negi et al., 2020) used honeypot as a security tool to detect and prevent attacks or exploits in the cloud. A proposed system was built to secure data and resource attacks in the cloud by detecting and monitoring user IP addresses. (Ryan Schukat, 2019) in their research used honeynets to track and profile WI-FI users. The honeynet devices developed for this study were made up of Raspberry Pi 3 B+, a battery power pack and USB WI-FI dongle. Privacy protection is a major security issue identified with this system. Device users will have their privacy compromised as information retrieved can be used to target advertisement etc. Using honeynet technology, a preventive defence mechanism against distributed denial of service (DDOS) attacks was proposed by (X. Wang et al., 2019). The system adopts an improved version of honeynet (unpatched Windows 2000 or Windows XP) that uses a multi-level data control mechanism on honeywall. The multi-level control mechanisms include IPTables, snort and Sebek for the capture attack behaviours.

2.4 DIGITAL FORENSICS (DF) AND DIGITAL FORENSIC READINESS (DFR)

The growing use of technology called for the employment of Digital Forensics (DF) to ensure the effective collection and storage of evidence which can be used and presented during an investigation. (A. K. Kyaw et al., 2020) defines DF as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations." In the DF process, digital forensic investigation (DFI) has served as a post-incident response during an incident or breach. The effectiveness of DF therefore called for the preparedness for an incident to occur thereby enabling organizations to efficiently gather and rely on digital evidence. The introduction of digital forensic readiness (DFR) as an incident preparedness seeks to efficiently maximise the potential use of digital evidence when required (Rowlingson Ph, 2004). DFR is an incident anticipation whiles DFI involves incident response. DFR is a process-oriented model which can serve as an investigation standard for civil, criminal and enterprise.

The processes involved in DFR differentiates from DFI and are presented in a circular, redundant hierarchy as shown in Figure 1. A DFR framework shall include (Mouhtaropoulos et al., 2013). In a DFR process model, three foundations (administrative, technical, and physical) are to be established to support activities and tasks to be performed in all phases of the model (Sachowski, 2016). DFR can cause privacy issues which can therefore be dealt with if an effective privacy policy is adopted to prevent legal issues. Activities and steps in Figure 1 are modelled into Figure 2. Discussed below are some models that have been proposed over the years to ensure digital forensic readiness. (Valjarevic Venter, 2011)proposed a DFR model for PKI which aims to preserve or improve Information systems security in PKI systems. The DFR model based on the ISO/IEC 27001:2013 was employed as a foundation to secure information systems environments (Kazadi Jazri, 2015).

This model is made up of four phases: Readiness, Collection, Storage and Deletion. (Ikuesan Venter, 2017) recommended a DFR framework for behavioural biometrics by using the ISO/IEC 27043 standard. The behavioral biometrics-based digital forensics readiness framework (BBDFRF) seeks to integrate behavioral biometrics into proactive forensics. The implementation of a DFR (Ros, 2018) to detect suspicious activities and transmit collected data in a "forensically sound manner". (Kebande et al., 2016) suggested an innovative DFR framework using the honeypot technology to capture, preserve and store potential digital evidence (PDE). The honeyd agent is used for monitoring, logging, and preserving PDE. Another DFR framework proposed was by (A. Kyaw et al., 2019) to mitigate security vulnerabilities and failure in existing IoT medical devices and wireless networks. The framework is made up of these components: Pi-drone, Wireless Forensic Server (WFS), Remote Authentication Dial-In User Service (RADIUS) Server, Wireless Access Point (WAP) Controller, Integrity Checking/Hashing Server (OSSEC), Intrusion Detection/Prevention System (Bro-IDS) Server, Web Server (XAMPP), and a centralised Syslog Server (Splunk). (Singh et al., 2019) proposed a DFR mechanism which complies with ISO/IEC 27043 standard to mitigate ransomware attacks.

3. PROPOSING DIGITAL FORENSIC READINESS FRAMEWORK FOR BYOD USING HONEYPOT AND HONEYNET

There is little investigation in digital forensic readiness for BYOD environments. Most frameworks proposed are focused on some aspects of BYOD. (Kebande et al., 2016)

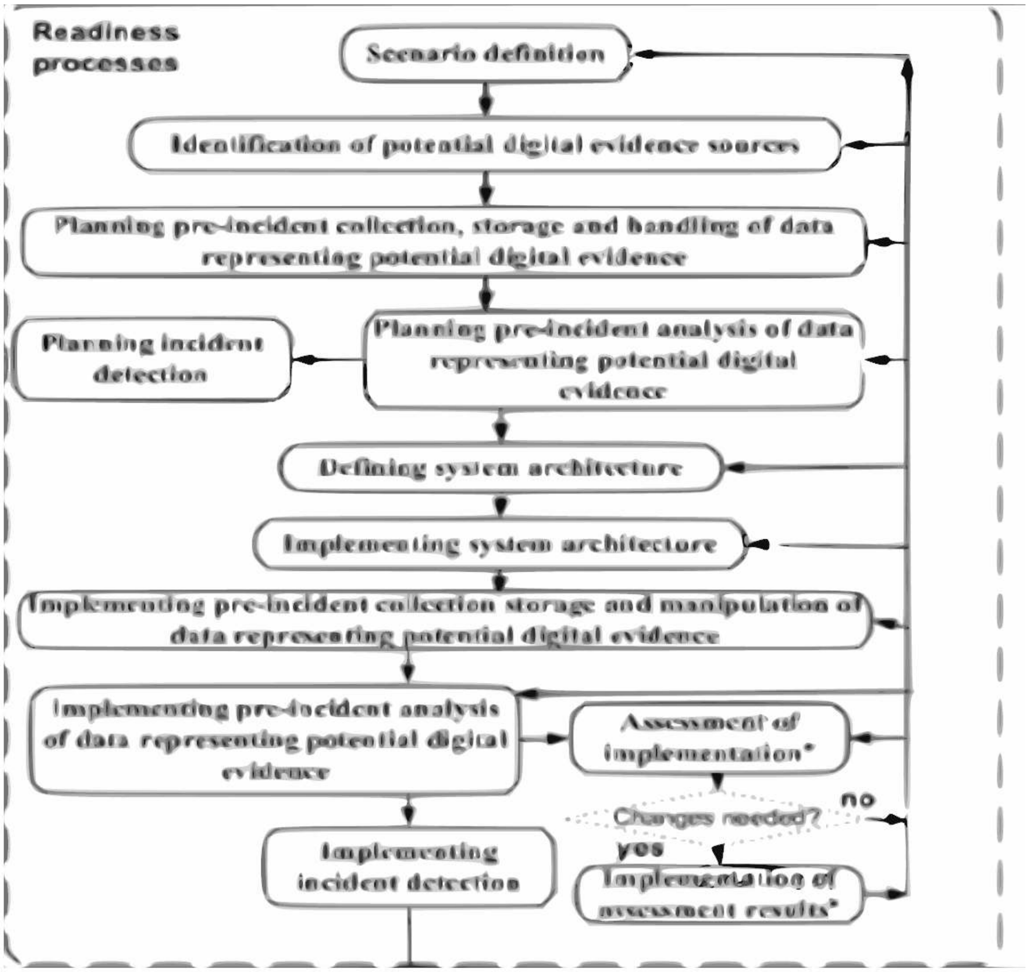

Readiness processes
Scenario definition
Identification of potential digital evidence sources
Planning pre-incident collection, storage and handling of data representing potential digital evidence
Planning incident detection
Planning pre-incident analysis of data representing potential digital evidence
Defining system architecture
Implementing system architecture
Implementing pre-incident collection storage and manipulation of data representing potential digital evidence
Implementing pre-incident analysis of data representing potential digital evidence
Assessment of implementation*
Changes needed?
no
yes
Implementing incident detection
Implementation of assessment results*

Figure 1. Digital Forensic Readiness model Source: (Valjarevic et al., 2017)

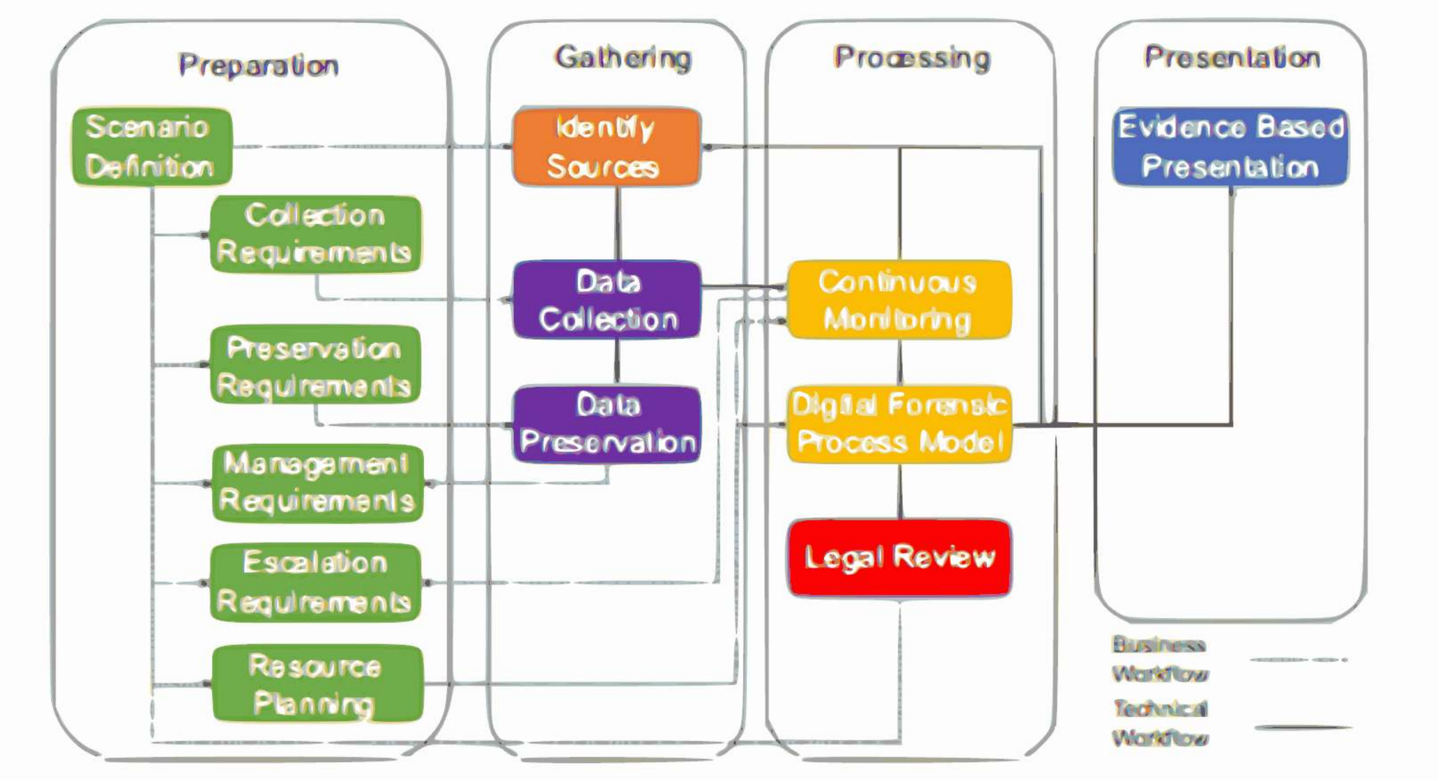


Figure 2. High-Level Digital Forensic Readiness model Source: (Sachowski, 2016)

in their work, proposed a DFR model that aimed to collect honeyd logs as potential digital evidence (PDE) using a honeyd honeypot which will act as a decoy agent. This model comprises of five components: BYOD Management, BYOD Technology, Honeyd agent, People, Forensic Readiness and the Digital Forensic Investigation (DFI) process. This model complying with ISO/IEC 27043 produces an innovative means of collecting potential digital evidence. The limitation of this model is its ineffectiveness of detecting security incidents. The implementation of honeyd, a low interaction honeypot, limits the identification and collection of potential security incidents in a BYOD environment.

3.1 Framework Overview

The proposed framework designed complies with ISO/IEC 27043 and aimed at detecting security incidents and collecting potential digital evidence using honeypot technology. It is also aimed at minimizing digital forensic investigation cost, maximizing the potential use of digital evidence gathered, preserving, and improving information security (Sachowski, 2016). Well-known BYOD security models were adopted to establish dynamic and effective framework when implemented in small or large organizations. Based on four components illustrated in Figure 3, the proposed DFR framework for BYOD enhances the existing forensic readiness procedures for BYOD. It also enables the introduction of new forensic technologies by organizations when adopted.

3.2 Proposed DFR framework for BYOD

The proposed DFR framework for BYOD is illustrated in Figure 4. The five components of the framework are discussed below:

- BYOD Devices BYOD Device management includes the identification of BYOD device types to be incorporated in an organization and the provision of security solutions for these BYOD Devices. All approved BYOD device types to be used are required to be registered to ensure the management and monitoring of activities. Providing a security solution requires the creation of personal space and corporate space on BYOD Devices. Space isolation provides the application of different security policies for BYOD Devices (Y. Wang et al., 2014). In this context, applications can be controlled, and security provided for corporate data. It also ensures the creation of a trusted platform for monitoring the activities of users and applications, as well as user identity management. Existing device management security solutions in an organization will be evaluated to provide the necessary support in creating a trusted platform for the monitoring of activities in the organization. In compliance with the organization's policies, a standard can be developed in handling BYODs. BYOD device management is aligned with the policies of the organization.

- Management BYOD management domain ensures the development and implementation of security controls and levels for BYOD in an organization. This domain certifies BYOD programs and policies as well as overseeing and monitoring of approved policies and BYOD usage. All risk management and assessments are to be performed as to provide an effective implementation of BYOD in an organization. In this domain, top management is to oversee the governance of BYOD devices, users, and technology. Legal and regulatory requirements are to be established in addition to other policies in the organization. The IT de-

Management
Technology
[Forensic Readiness]
People
BYOD Devices

Figure 3. High-Level Digital Forensic Readiness model Source: (Sachowski, 2016)

partment is to manage and provide applications and services to users within the organization. They are also to enforce the usage of BYOD to follow approved policies established in the organization.

- People People are authorized users in an organization. Eligible users should be authorized to access corporate resources while connected to the organization's network. Implementation of the Service Level Agreement (SLA) can allow organizations to legally track user activities and proactively gather digital evidence for civil, criminal, or corporate investigations.

- Technology This domain consists of policy database, access control, corporate resources, mobile device management (MDM) system, honeypot technology and DFR. The policy database should have well-defined policies that will allow organizations to collect and examine digital evidence as well as conduct investigations with potential digital evidence. In compliance with the organization's policies, all access to corporate resources are to be monitored and recorded. User access to corporate resources through their BYOD devices should be controlled and managed by network access control and MDM. MDM, which collects management information and enforces policies, will serve as an enforcer for users to allow them to comply with policies and to monitor activities. Network access control in granting access requests to corporate resource should direct user activities to be monitored by honeypot technologies. The implementation and enforcement of policies must guide users in the organization by creating the awareness of their actions and activities. Honeypot technologies employed in this framework are to gather potential digital forensic information. In acquiring more information and identifying potential threats will require the implementation of more honeypots. Based on honeypots and honeynets evaluated in (Cabaj, 2015; Dalamagkas et al., 2019; Nawrocki et al., 2016; Velasco Silva Rodríguez Rafael, 2017), recommended honeypots suitable to be implemented will be: Low: Dionaea, HoneyDroid, Cowrie, Glastopf, BOF, DTK, HoneyBot, GHH, Thug High: Argos, Sebek, HoneySpider Information gathered from honeypot technologies are to be stored in forensic, profile and log files databases. Organizations can also select the appropriate honeypots to enable customize their honeypots needed for the implementation of the framework.

- DFR Forensic readiness model depicted in Figure 2 has been grouped into four phases: preparation, gathering, processing and presentation.

- Preparation All scenarios are to be examined whereby there will be the need for digital evidence. Risks involving threats/vulnerabilities are to be assessed to identify the necessary actions to achieve DFR and information security.

- Gathering Potential digital evidence or forensic information will be gathered from BYOD devices, honeypot technologies, corporate resources and MDM. Logs and profile information will be gathered from the sources listed above. Data collection tools used in honeynets explained in (Velasco Silva Rodríguez Rafael, 2017) will also serve in gathering potential digital evidence. Acquisition and analysis of digital evidence or forensic information to be relied on during an investigation should comply with the correct forensic data acquisition procedures. Potential digital evidence collected are to be preserved through hashing and encryption to ensure integrity before storing in the evidence database. Time synchronization is crucial in synchronizing evidence collected from the different honeypots implemented in the framework. This feature is important in identifying the correct time an incident occurred. All evidence from incidents are to be validated and normalized before storage in forensic, profile and log files databases.

- Processing To potentially gather forensic information requires the constant monitoring of an organization's network. Monitoring involves the collection of logs, traffic, detection of vulnerabilities, attacks, techniques, methods, and motivation of attackers. The constant review of gathered forensic information can help shape and audit policies in an organization. Digital evidence stored in the evidence database will be relied upon and used during a forensic investigation. Access to evidence data stored requires authorization and authentication. Effective legal analysis should be carried out to provide a response to accidents in the company.

- Presentation This phase involves report documentation and presentation of processes and findings during a digital forensic investigation. The required documentation report can support decision making, legal and administrative measures.

- EVALUATION Evaluating the proposed framework requires an alignment with the ISO/IEC 27043 standard. In developing a DFR framework, it is essential to identify and implement all the necessary processes identified in the ISO/IEC 27043 standard. The proposed framework is developed to integrate all the essential processes in DFR. The proposed DFR framework for BYOD can be evaluated by mapping the processes to the ISO/IEC 27043 standard processes.

The framework proposed in this study contributes to the field of BYOD and digital forensics. It has a wider scope as compared to previously proposed frameworks. It incorporates both security and digital forensic readiness in a BYOD environment. The framework can be used to implement security and DFR in organizations who already have BYOD technology instituted. Organizations who intend to adopt BYOD can also depend on this framework to secure their organizations and have an intrinsic digital forensic readiness component. This framework would also allow researchers and developers to create enhanced security solutions

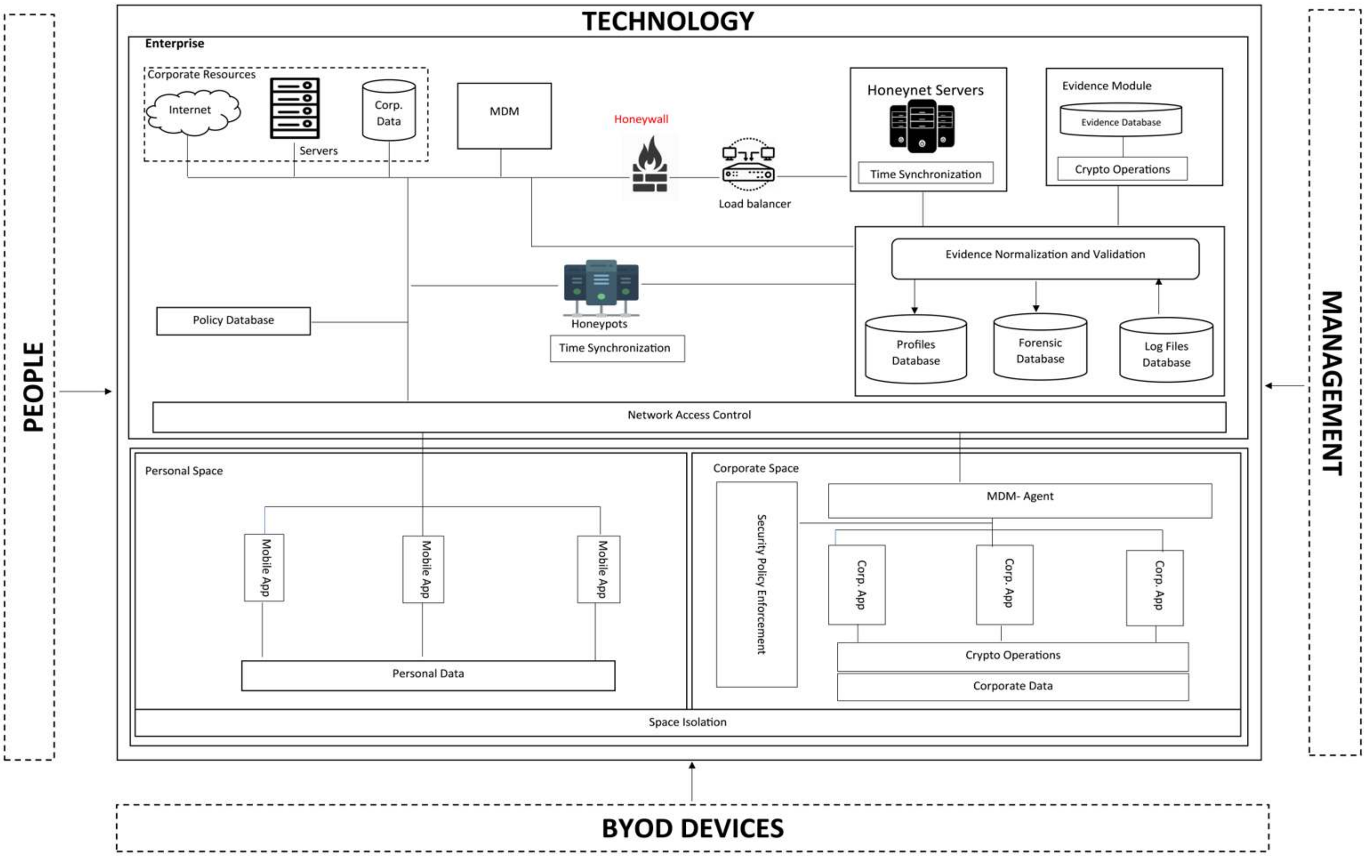
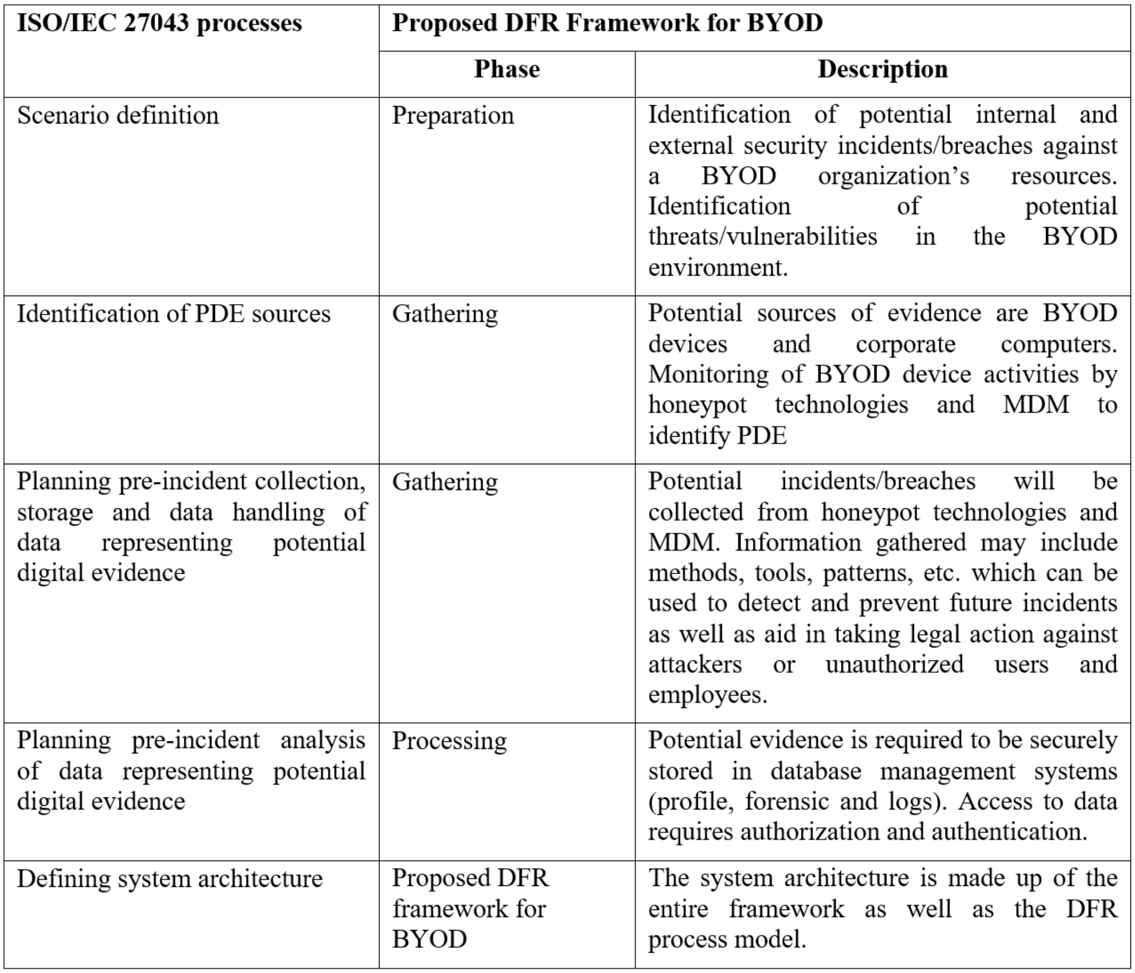


Figure 4. DFR Framework for BYOD



ISO/IEC 27043 processes	**Proposed DFR Framework for BYOD**	
	Phase	**Description**
Scenario definition	Preparation	Identification of potential internal and external security incidents/breaches against a BYOD organization's resources. Identification of potential threats/vulnerabilities in the BYOD environment.
Identification of PDE sources	Gathering	Potential sources of evidence are BYOD devices and corporate computers. Monitoring of BYOD device activities by honeypot technologies and MDM to identify PDE
Planning pre-incident collection, storage and data handling of data representing potential digital evidence	Gathering	Potential incidents/breaches will be collected from honeypot technologies and MDM. Information gathered may include methods, tools, patterns, etc. which can be used to detect and prevent future incidents as well as aid in taking legal action against attackers or unauthorized users and employees.
Planning pre-incident analysis of data representing potential digital evidence	Processing	Potential evidence is required to be securely stored in database management systems (profile, forensic and logs). Access to data requires authorization and authentication.
Defining system architecture	Proposed DFR framework for BYOD	The system architecture is made up of the entire framework as well as the DFR process model.

Table 1. Proposed DFR Framework Evaluation

that can identify potential threats and vulnerabilities an organization will encounter. It can also be relied on to create a platform that can incorporate security and DFR into an organization.

In gathering more evidence, low and high interaction honeypots were incorporated into this framework. The framework, which not only acts as a potential digital evidence capturing tool, also helps during a digital forensic investigation. It ensures the provision of evidence from actions, events, and processes in the BYOD environment. To prevent inconsistent recording of incidents/threats identified by the honeypots, time synchronization has been introduced. Preservation of digital evidence, which is an important step in the forensic investigation, is catered for in this framework and access to preserved evidence requires authorization before obtaining it for analysis.

The proposed framework includes profiling. Profiling is key during a forensic investigation. It helps to narrow down an investigation and understand the motives of a crime. The patterns obtained during an investigation are used to establish a general description of the suspects. Profiling helps to assist investigators and security personnel when deducing potential suspects, predicting future criminal activities. The adoption of profiling in this framework will help organizations and investigators to develop better investigative search strategies.

This study is a contribution to enhancing security and digital forensic readiness into a BYOD organization.

4. CONCLUSION

This paper identifies the need for organizations who adopt BYOD because of its benefits to be prepared for the challenges it poses and the need to provide or improve security and be forensically prepared to gather digital evidence which can protect the organization against legal and technical incidents. A digital forensic readiness framework for a BYOD environment was therefore proposed in this study. As BYOD environments are prone to security threats and challenges, implementation of such framework will significantly improve information security and provide reliable digital evidence for forensic investigation. This framework can easily be implemented in an existing BYOD network or adopted by organizations who intend to accept BYOD technology in their working environment. The improved model incorporates high and low interaction honeypots to detect security incidents and collect digital evidence. The proposed framework will enable organizations to embed digital forensic readiness in a BYOD security solution. This framework will not only be cost effective but also provide a trusted platform for employees in the organization. For future work, the proposed DFR BYOD framework would have to be implemented and tested in a BYOD environment. More procedures will be evaluated during the implementation of the framework.

REFERENCES

[1] Agnaou, A., Kalam, A. A. El, Ouahman, A. A. (2018). Towards a collaborative architecture of honeypots. Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA, 2017-October. https://doi.org/10.1109/AICCSA.2017.208

[2] Ahmad, A., Webb, J., Desouza, K. C., Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. In Computers and Security (Vol. 86). https://doi.org/10.1016/j.cose.2019.07.001

[3] Cabaj, K. (2015). HoneyPot systems in practice. PRZEGLD ELEKTROTECHNICZNY, 1(2). https://doi.org/10.15199/48.2015.02.16

[4] Chamotra, S., Sehgal, R. K., Ror, S. (2016). Bot detection and Botnet tracking in Honeynet context. Smart Innovation, Systems and Technologies, 50. https://doi.org/10.1007/978-3-319-30933-0_56

[5] Dalamagkas, C., Sarigiannidis, P., Ioannidis, D., Iturbe, E., Nikolis, O., Ramos, F., Rios, E., Sarigiannidis, A., Tzovaras, D. (2019). A Survey on honeypots, honeynets and their applications on smart grid. Proceedings of the 2019 IEEE Conference on Network Softwarization: Unleashing the Power of Network Softwarization, NetSoft 2019. https://doi.org/10.1109 /NETSOFT.2019.8806693

[6] Downer, K., Bhattacharya, M. (2015). BYOD security: A new business challenge. 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), 1128–1133.

[7] Gonzalez, C., Aggarwal, P., Lebiere, C., Cranford, E. (2020). Design of Dynamic and Personalized Deception: A Research Framework and New Insights. Proceedings of the 53rd Hawaii International Conference on System Sciences. https://doi.org/10.24251/hicss.2020.226

[8] Gudo, M., Padayachee, K. (2015). SpotMal: A hybrid malware detection framework with privacy protection for BYOD. ACM International Conference Proceeding Series, 28-30-September-2015. https://doi.org/10.1145/2815782.2815812

[9] Ikuesan, A. R., Venter, H. S. (2017). Digital forensic readiness framework based on behavioral-biometrics for user attribution. 2017 IEEE Conference on Applications, Information and Network Security, AINS 2017, 2018-January. https://doi.org/ 10.1109/ AINS.2017.8270424

[10] Kazadi, J. M., Jazri, H. (2015). Using digital forensic readiness model to increase the forensic readiness of a computer system. Proceedings of 2015 International Conference on Emerging Trends in Networks and Computer Communications, ETNCC 2015. https://doi.org/ 10.1109/ETNCC.2015.7184822

[11] Kebande, V. R., Karie, N. M., Venter, H. S. (2016). A generic Digital Forensic Readiness model for BYOD using honeypot technology. 2016 IST-Africa Conference, IST-Africa 2016. https://doi.org/10.1109/ ISTAFRICA.2016.7530590

[12] Kyaw, A., Cusack, B., Lutui, R. (2019). Digital Forensic Readiness in Wireless Medical Systems. 2019 29th International Telecommunication Networks and Applications Conference, ITNAC 2019. https://doi.org/ 10.1109/ITNAC46935.2019.9078005

[13] Kyaw, A. K., Tian, Z., Cusack, B. (2020). Design and Evaluation for Digital Forensic Ready Wireless Medical Systems. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, 314 LNICST. https://doi.org/10.1007/978-3-030-42029-1_9

[14] Martin, V., Cao, Q., Benson, T. (2017). Fending off IoT-hunting attacks at home networks. CAN 2017 - Proceedings

of the 2017 Cloud-Assisted Networking Workshop, Part of CoNext 2017. https://doi.org/10.1145/3155921.3160640

[15] Mouhtaropoulos, A., Dimotikalis, P., Li, C. T. (2013). Applying a Digital forensic readiness framework: Three case studies. 2013 IEEE International Conference on Technologies for Homeland Security, HST 2013. https://doi.org/10.1109/THS.2013.6699003

[16] Nawrocki, M., Wählisch, M., Schmidt, T. C., Keil, C., Schönfelder, J. (2016). A survey on honeypot software and data analysis. ArXiv Preprint ArXiv:1608.06249.

[17] Negi, P. S., Garg, A., Lal, R. (2020). Intrusion detection and prevention using honeypot network for cloud security. Proceedings of the Confluence 2020 - 10th International Conference on Cloud Computing, Data Science and Engineering. https://doi.org/10.1109/ Confluence47617.2020.9057961

[18] Pawlick, J., Nguyen, T. T. H., Colbert, E., Zhu, Q. (2020). Optimal Timing in Dynamic and Robust Attacker Engagement During Advanced Persistent Threats. `https://doi.org/10.23919/wiopt47501.2019.9144123`

[19] Pickett, M. (2003). A Guide to the honeypot concept. Sans Institute.

[20] Ratchford, M. M., Wang, Y. (2019). Byod-insure: A security assessment model for enterprise byod. 2019 5th International Conference on Mobile and Secure Services, MOBISECSERV 2019. https://doi.org/10.1109/ MOBISECSERV.2019.8686551

[21] Ros, E. (2018). Digital Forensic Readiness in Mobile Device Management Systems. University of Pretoria.

[22] Rowlingson, R. (2004). A ten step process for forensic readiness. International Journal of Digital Evidence, 2(3), 1-28.

[23] Ryan, F., Schukat, M. (2019). Wi-fi user profiling via access point honeynets. 30th Irish Signals and Systems Conference, ISSC 2019. https://doi.org/10.1109/ISSC.2019.8904968

[24] Sachowski, J. (2016). Investigative Process Models. In Implementing Digital Forensic Readiness. https://doi.org/10.1016/ b978-0-12-804454-4.00002-2

[25] Simmons, R., Vandeven, S. (2017). BYOD Security Implementation for Small Organizations. SANS Institute InfoSec Reading Room.

[26] Singh, A., Ikuesan, A. R., Venter, H. S. (2019). Digital Forensic Readiness Framework for Ransomware Investigation. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, 259. https://doi.org/10.1007/978-3-030-05487-8_5

[27] Spitzner, L. (2003). Honeypots: tracking hackers (Vol. 1). Reading: Addison-Wesley.

[28] Valjarevic, A., Venter, H., Petrovic, R. (2017). ISO/IEC 27043:2015 - Role and application. 24th Telecommunications Forum, TELFOR 2016. https://doi.org/10.1109/TELFOR.2016.7818718

[29] Valjarevic, A., Venter, H. S. (2011). Towards a digital forensic readiness framework for public key

infrastructure systems. 2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference. https://doi.org/10.1109/ ISSA.2011.6027536

[30] Velasco Silva, D., Rodríguez Rafael, G. D. (2017). A review of the current state of Honeynet architectures and tools. International Journal of Security and Networks, 12(4). https://doi.org/10.1504/ ijsn.2017.10009165

[31] Vignesh, U., Asha, S. (2015). Modifying security policies towards BYOD. Procedia Computer Science, 50. https://doi.org/10.1016/ j.procs.2015.04.023

[32] Wang, X., Guo, N., Gao, F., Feng, J. (2019). Distributed denial of service attack defence simulation based on honeynet technology. Journal of Ambient Intelligence and Humanized Computing. https://doi.org/10.1007/ s12652-019-01396-x

[33] Wang, Y., Wei, J., Vangury, K. (2014). Bring your own device security issues and challenges. 2014 IEEE 11th Consumer Communications and Networking Conference, CCNC 2014. https://doi.org/10.1109/ CCNC.2014.6866552