IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A REVIEW OF CYBER-CRIME IN INTERNET OF THINGS: TECHNOLOGIES, INVESTIGATION METHODS AND DIGITAL FORENSICS

Dr. Algimantas Venčkauskas*, Dr. Robertas Damaševičius, Dr. Vacius Jusas, Dr. Jevgenijus Toldinas, MSc Darius Rudzika, MSc Giedrė Drėgvaitė
* Computer Science Department, Kaunas University of Technology, Kaunas, Lithuania

ABSTRACT

The Internet of Things (IoT) is a novel design paradigm, which allows communication among different kinds of physical objects over the common Internet infrastructure. Operations and application models of the IoT, which differ from the traditional networks, have brought great challenges and opportunities to digital forensic technology. In this paper we analyse the state of cybercrime in the IoT, current methods and tools of digital forensics readiness and investigation and possibilities of their application for the investigation of cybercrime in the IoT.

KEYWORDS: cybercrime, digital forensics, Internet of Things.

INTRODUCTION

The Internet of Things (IoT) is a novel-networking paradigm, which allows communication among all types of physical objects (or "things") over the Internet [1]. A thing is an entity or a physical object, which has a unique identifier and can transfer data over the network. The IoT defines a worldwide cyber-physical system [2] with a multitude of applications, including domestics, e-health, tracking of goods and logistics. It has been developed on the basis of wireless technologies, micro-electromechanical systems and the Internet technology.

In terms of technical standardization, IoT can be understood as a global networking infrastructure for the information society enabling provision of advanced services by interconnecting physical and virtual things based on the existing and evolving networking infrastructure as well as information and communication technologies.

In 2011, the number of networked devices overtook the total global human population [3]. It is anticipated that by 2020, the number of devices connected to the IoT may outnumber the number of connected people by the ratio of six to one, transforming the current Internet into the Internet of Things. In the highly interconnected world of tomorrow, in the Future Internet, it will become difficult to imagine any crime that does not involve digital evidence linked with the IoT. Operations and application models of the IoT are different from the traditional networks, which have brought great challenges and opportunities to digital forensic technology.

The paper aims to overview and analyse the specifics of a cybercrime in the IoT, existing methods and tools of digital forensics readiness and investigation and possibilities of their application for the investigation of a cybercrime in the IoT.

The manuscript is structured as follows. Section 2 discusses dangers of the IoT, presents a taxonomy of cybercrimes, formulates security challenges and requirements for the IoT, discusses security features, specific attacks and threats to the IoT, and outlines cybercrime trends for the IoT. Section 3 provides an overview of the investigation methods and their applicability to the IoT, discusses the existing methods of the digital forensics readiness of an organization in the context of the IoT, and enlists challenges and recommendations for digital forensics investigations carried out in the IoT environments. In Section 4 conclusions are given.

CYBERCRIMES IN THE IoT

Dangers of the IoT

The development of the IoT is likely to lead to a variety of ethical problems and discussions in society. Many of these, such as the loss of confidence, privacy violations, misuse of data, the digital divide, identity theft, access to information and control problems, freedom of speech and freedom of expression, have already arisen in connection with the use of the Internet and ICT in general. However, with the development of the IoT many of these problems have become more important.

Privacy aspects. People's privacy and the confidentiality of business processes [4] are two main issues associated with the IoT. Security and privacy issues are raised when an identifiable 'thing' meets 'the subject', i.e., the Internet user [5]. The massive use of the IoT, mobility of things and sometimes their relatively low complexity, makes the IoT to be difficult to control. For the issue of confidentiality, encryption technology has been developed, and one of the main challenges is to make encryption/decryption algorithms faster and less energy-consuming for the resource-constrained IoT devices.

Regarding privacy, the situation is more serious; the ignorance of the general public privacy questions is one of the reasons. Also, privacy-preserving and enhancing technologies are still in their infancy: the systems that realise it have not been designed for the resource-restricted devices, and a holistic approach on privacy have not been developed yet. New concepts such as *Privacy by Design* have to be investigated and implemented.

The following privacy and data protection issues related to the IoT [6]:

Continuity and availability of services: The issue of continuity and availability of the services rises with spreading the deployment of the IoT and more and more systems and people relying on these new products, applications and services. The integration of the IoT devices in our everyday lives, and especially in critical services (such as health, security, and energy) increase the impact of a potential loss of a service.

User data sensibility: Smart services gather more and more information on the user (willingly or even without notice), therefore the question of the sensibility of these data arise. Due to an increasing amount of information the IoT makes this issue complicated. The actual sensibility of gathered information is not always known at the time when data gathering is decided. In the IoT risks related to privacy and data security are dependant on the context and purpose under which data are gathered and used. So the context-aware management of the security and data protection is needed.

User data security: The user data must be protected against unauthorized access, and this security should be ensured at each level of communication. The variety of the IoT devices and an increasing number of characteristic links, therefore, makes this protection complicated. The potential impact of security breaches is also rising as the data stored have more and more applications, and thus provide more and more information on the user and give more and more access to critical parts of our lives.

Data management: Even when the security of the user data can be guaranteed against unauthorized access, the question of the actual management and storage of the information by the service provider remains.

Ownership and repurposing of data: The question of the ownership of the data collected is also important in relation to the issue of the IoT ethics: getting propriety or access to user data and reselling these data can be a source of revenue.

Data captivity: Though the service is becoming more and more used by the user, the ethical questions (what happens to the user data if the user leaves the service and how feasible is it for a customer to change service provider which provided the service for a long time) remain unanswered. These questions are important to avoid consumer captivity through data that would result in an unfair advantage, destroying competition, suppression of a consumer choice, degradation of a user service, and decrease in innovation.

Applicable legislation: In respect to the global nature of the IoT and the number of stakeholders necessarily involved in the IoT deployment, the question of responsibility and applicable legislation arise. This is confirmed by the fact that different actors of the IoT will be spread across different countries and regions, increasing the number of the potential legislation involved. This question is important not only for users, which may be confused on which legislation they follow, but also for policy makers and the whole IoT value chain as the developing IoT applications and deployment without a clearly identified chain of responsibilities and applicable law represent strong business risks.

Availability of information: the service provider must ensure that not only the information is available, but that it is presented in a way that is properly understood by the user.

User traceability: Security mechanisms should prevent the traceability of users throughout the entire network, which, in turn, may harm end user privacy by providing data to the attacker that can be analysed intending to define behaviour patterns of the user [7].

All these concerns lead to the so called 'privacy paradox' [8]: by collecting personal data, better "personalized" services can be offered to users; but these personal data can be processed by data mining techniques and assembled into user profiles, which may be detailed enough to allow user identification. When these "personal data" have been disclosed, the owner of the data cannot control how the data collector will use it. If so, a question arises if the user should be able to refuse to disclose personal information and at the same time to refuse life-enhancing services.

Security aspects. Computer security includes all the processes and mechanisms that protect computer equipment, information and services from accidental or unauthorized access, modification or destruction. The following security issues related to the IoT [9]: a) the security architecture, which describes the system elements responsible for the security management during the lifecycle of a thing; b) the security model of a node, which describes how security parameters, processes, and applications are managed in a thing; c) security bootstrapping, which defines how a thing can securely join the IoT at a given location and point in time; d) network security, which describes the mechanisms applied within a network to ensure trusted operation of the IoT; and e) application security, which guarantees that only trusted objects can communicate with each other.

Computer network security consists of the precautions taken for the prevention of unauthorized access, misuse, modification, blocking a computer and network resources available via the network. Network security includes network access data authorization, which is managed by the network administrator. The Internet is an insecure channel for the exchange of information, which leads to a high risk of fraud or intrusion. The IoT is based on computer networks and the Internet to maintain connection between objects, as well as between people and things. Therefore, it is relevant to all of the computer network and Internet security issues. Before using smart chips, companies and public authorities should assess their impact on privacy and data protection. On the basis of these assessments certified by national data protection authorities, personal data security and trusted security should be ensured.

Definitions and typology of a cybercrime

Like traditional crime, a cybercrime has many different facets and may occur in a wide variety of scenarios. Existing definitions of a cybercrime differ depending on the perspective of a victim, protector and observer. Newman [10] defines cybercrime as a behaviour in which computers or computer networks are a tool, a target, or a place of criminal activity. This includes both means and techniques to commit attacks on information assets as well as the use of computers to commit a "traditional" crime. The Council of Europe's Cybercrime Treaty uses the term "cybercrime" to describe different offences starting from criminal activity against data to content and copyright infringement [11]. The 'Manual on the Prevention and Control of Computer Related Crime' by the United Nations also includes unauthorized access, fraud and forgery [12] in its definition of a cybercrime. Gordon and Ford [13] define cybercrime as "any crime that is facilitated or committed using a computer, network, or hardware device".

The Council of Europe's Convention on Cybercrime postulates four different types of offences: 1) Offences against integrity, confidentiality, and availability of computer data and computer systems; 2) Computer-related offences; 3) Content-related offences; and 4) Copyright-related offences. This classification is inconsistent as there is some overlap between categories [14].

Saini *et al.* [15] categorize cybercrimes as follows:

Data crimes include data interception (an attacker monitors data streams to or from a target in order to gather information), data modification (interception of data in transit and modification of parts of that data before retransmitting it) and data theft (illegal copy or theft of data from a business or other individual).

Network crimes enclose interfering with the functions of a computer network by inputting, transmitting, damaging, modifying or suppressing network data.

Access crimes refer to unauthorized access and virus dissemination.

Content-related crimes such as violations of copyright, unsolicited commercial messaging, and cyber threats.

Zhang *et al.* [16] categorize cybercrimes as crimes in which 1) the computer or network is used mainly as tools, including spamming and criminal copyright violations, (2) the computer or network is the target of a criminal activity, including unauthorized access, malware, and hacking, (3) the computer or network is the location of a criminal activity, e. g., financial frauds, (4) traditional crimes facilitated through computers or networks, e. g., harassment, (5) other information crimes facilitated by computers or networks, such as theft.

Cybercrime has evolved from traditional crimes (such as fraud) as a consequence of the technological progress, which has enlarged the conventional crime space by providing more (sophisticated) means, more opportunity and new action grounds and targets [17]. In terms of general means, the Information and Communication Technologies (ICT) increase both for speed and reach of criminal activities. Opportunity is often seen as another crucial element or even as a primary provoking agent in triggering of a criminal act [18]. The Internet itself is an opportunity-rich environment for criminal activities as it was not originally designed having security in mind. As the IoT is built on top of the existing Internet infrastructure, the problems related with a cybercrime remain as relevant as ever or even grow in size as more nodes and services are connected anytime-anywhere, thus, the gap between accelerating criminal opportunities versus diminishing control keeps growing [19]. In addition to the increased availability of criminal targets, the IoT also amplifies opportunities to access information, tools and support to execute misdemeanours. Finally, a vast dimension and complexity of the cyber context provides opportunities to conceal offences from public due to the virtual nature of the criminal methods.

Computer crime concerns and challenges in the IoT

The Internet of Things (IoT) poses new challenges to the protection of data and end-user privacy [14]: users will be unwilling to adopt the IoT that invisibly blends into their living environment without being assured that safety of private information is guaranteed and adequate security is provided. Connecting every 'thing' in the global Internet infrastructure and having 'things' communicating with each other, new security and privacy problems, e.g., confidentiality, authenticity, and integrity of data sensed and exchanged by 'things' [20] are to arise. The security of humans and things in the IoT must be ensured to prevent and fight cybercrimes.

General security requirements for the IoT are summarized in Table 1 (based on [21]). The following basic security properties for the IoT must apply in order to prevent a computer crime [22]:

Confidentiality: the protection of information; ensures that transmitted data can be read only by the communication endpoints;

Availability: the communication endpoints can always be reached and cannot be made inaccessible; information is always available when required.

Integrity: ensures that received data are not tampered with during transmission; if this does not happen, then any change can be detected;

Authentication: the prevention of the unauthorized node use, i.e. making sure nodes are not compromised, data sender can always be verified and data receivers cannot be spoofed. Authentication involves mutual verification of routing peers before they share route information and ensures shared data origin is accurate. Authentication can require significant time and efforts from end users and therefore needs to be optimized as far as possible [23].

Table 1. General security requirements for the IoT

Requirement	Description
Resilience to attacks	The system has to avoid single points of failure and should adjust itself to node failures
Data authentication	Retrieved address and object information must be authenticated
Access control	Information providers must be able to implement access control on the data provided
Client privacy	Measures need to be taken that only the information provider is able to infer from observing the use of the lookup system related to a specific customer; at least, inference should be very hard to conduct
User identification	The process of validating users before allowing them to use the system
Secure storage	Involves confidentiality and integrity of sensitive information stored in the system
Identity Management	Identifying individuals / things in a system and controlling their access to resources within that system by associating user rights and restrictions with the established identity
Secure data communication	Authenticating communicating peers, ensuring confidentiality and integrity of communicated data, preventing repudiation of a communication transaction, and protecting the identity of communicating entities
Availability	Ensuring that unauthorized persons or systems cannot deny access or use to authorize users
Secure network access	Provides a network connection or service access only if the device is authorized
Secure content	Content security or Digital Rights Management (DRM) protects the rights of the digital content used in the system
Secure execution environment	A secure, managed-code, runtime environment designed to protect against deviant applications
Tamper resistance	Maintain these security requirements even when the device falls into the hands of malicious parties, and can be physically or logically probed

Security threats and attacks in the IoT

A thing undergoes several stages in its lifecycle [24]. Most things usually go through manufacturing, installation, and operational. At each stage, different security and privacy concerns have to be addressed.

Manufacturing: IoT nodes usually are tailored towards specific tasks. Therefore, a network may contain nodes created by different manufacturers, some of them may be untrustworthy. An attack that could occur during this phase would involve an untrustworthy manufacturer that clones the device. In the worst-case, device software may be changed to implement harmful features [24].

Installation: During commissioning of a thing, the device identity and secret keys are provided, which will be used for communication during operation of a things. Attacks that may occur during the installation stage involve obtaining the secret keys when the installer provides them to the device [25]. If the attackers manage to obtain secret keys, then the IoT communications are severely compromised.

Operational attacks can be classified as physical capture, disrupt, degrade, deny, destruction, manipulation and eavesdropping attacks [22]. Considering the operational attacks, we can distinguish three main types of the attackers (based on [26]): 1) things with unintended behaviour due to hardware or software failures: problems caused by such faulty things should be solved by fault tolerance measures instead of the security ones; 2) external malicious things, which cannot access legitimately the IoT; 3) internal malicious things, which are a legitimate part of the IoT and have been captured or compromised by an attacker.

The threats to the IoT can also be categorized by the structural composition of the IoT. The structure of the IoT can be divided into four layers [27]: 1) **perceptual (physical) layer** gets information from the physical world using sensors for capturing and representing information in the digital world; 2) **Network layer** is responsible for the initial processing and reliable transmission of information received from the perceptual layer; 3) **Support (middleware) layer** sets up a liable support platform for the application layer, where all kinds of computing are organized through the network grid and cloud computing; and 4) **Application layer** provides user-personalized services.

Security features of each layer of the IoT can be summarized as follows [27]:

Physical layer: commonly, the IoT networks are centralized with many remotely located nodes, which may not have adequate protection from being captured. The attackers have opportunity to seize and extract security information from the device. This sort of attack can compromise the entire network. Networks can also experience disruption attacks at a physical layer if the attacker uses jamming or the interference equipment.

Perceptual layer: The perceptual layer is responsible for data collecting from external world. Sensor data need protection for integrity, authenticity and confidentiality. However, perceptual nodes usually are short of computer power and storage capacity, therefore, it is unable to apply a sophisticated security protection system. Node authentication is requiredto prevent from illegal node access; and data encryption is required to protect the confidentiality of messaging between the IoT nodes. However, stronger safety measures usually lead to higher level of resource consumption. The main threats mainly come from its wireless sensor network, RFID and mobile intelligent terminal security threats [28] such as physical capture, impersonation, and DoS attack.

Network layer: Security depends upon a core network. Since mass nodes are one of the major features of the IoT, mass nodes certification issues are one of the main challenges to be solved. The main security threat in the network layer consists of routing attacks such as malicious behaviour against right path topology and forwarding data, distributed DoS (DDoS) attacks, cyber-attacks across heterogeneous network, asynchronous attacks, collusion attacks and the middleperson attacks. Node impersonation attack allows for the access to a network as a legitimate node. Node resource spamming happens when a malicious node repeatedly joins a network aiming to drain the resources of the network and potentially shut down a portion of the network [29]. Confidentiality attacks aim to hijack routing information. To prevent against this exposure attack, all communicating nodes should be authenticated and the communication between nodes should be peer-to-peer [29]. Passive wiretapping attacks listen in on data sent between nodes. Unauthorized modification attacks aim to change information in a message or in the stored data. This type of an attack can be countered by adding access controls for storage and by implementing data integrity services for messages. Overclaiming and misclaiming attacks aim to change the topology of the network and routing data. This attack can be countered by restricting realizable network topologies. Spoofing attacks happen when an attacker tries to access a device by masquerading as someone else. These attacks can be encountered by using authentication controls. Routing information replay attacks happen when the attacker records and replays messages sent over the network back to the network aiming to disrupt operations. Selective forwarding attacks affect routing paths and aim to cause confusion within the network

[29]. Sinkhole attacks use a compromised node to advertise good links to attract traffic [24]. If sinkholes are coupled with selective forwarding, a portion of the network may be disabled. In overload attacks, a malicious node fills the network with random traffic aiming to deplete the energy resources of the network. These attacks can be resisted by adding limits on the traffic rate for each node [29]:

Support (middleware) layer: The IoT middleware layer mainly provides services for the basic tasks such as Web services and API (Application Program Interface). The challenge is to improve the ability to recognize malicious information using a stronger system security technology and anti-virus tools. The main threats that come from the support layer are the DoS attack, non-permission to access, data attacks, and session attacks.

Application layer: the main task of the application layer is to collect and process a large number of user data, including user's personal information or confidential information of various trades. So the data will become the attacker’s main attack target, stolen, tampered or damaged [28]. Different security needs for different applications apply, however, data sharing is the most common one, which causes problems related to the data privacy, disclosure of information, and access control. Other concerns are key agreement and authentication across the heterogeneous network, and information security management, especially password management. The attacker is likely to destroy privacy in the application layer by a known vulnerability (e.g., buffer overflow, cross site scripting, and SQL injection), error configuration (e.g., simple password), or improperly obtained higher permission access. The main threats are: privacy leak, DoS attack, malicious code, and social engineering.

The security threats in the IoT can be summarized as follows [24]:

1) threats that are related to the physical nature of smart objects, which are typically deployed in public areas and cannot be constantly supervised, thus leading to potential damages or counterfeits (e.g., cloning of smart things by untrusted manufacturers; malicious substitution of smart things during installation; firmware replacement attack; extraction of security parameters);

2) threats arising from the communication of things with each other (e.g., eavesdropping attack if the communication channel is not adequately protected; man-in-the-middle attack during key exchange; routing attacks; denial-of-service attacks);

3) threats arising from handling of personal or sensible data, which, if intercepted by unauthorized parties, may cause ethical and privacy problems.

4) Specific security threats for the IoT are summarised in Table 2.

Table 2. Specific security threats in the IoT

Cybercrime	Threat	Consequence
Data Crime	Node capture	IoT node physically compromised
Network Crime	Sinkhole attack	Attract the communication data to form a routing a black hole or selective forwarding
Network Crime	Sybil attack	Reduce the effectiveness of fault-tolerance mechanisms
Network Crime	Flooding attack	Keep broadcasting hello packets so that message would be lost because of a long distance
Access Crime	Impersonation attack	Intercepted legitimate ID or fake legitimate identity that lead to information disclosure
Network Crime	DOS attack	Blocking the communication channel, depleting the energy of IoT nodes
Network Crime	Replay attack	Gain access permission and decrease system‘s trust by replaying of the received messages
Data Crime	Spoofing attack	Disguise as a legitimate node to obtain data of tamper information

The analysis of crimes in the IoT

Fraud. In an example of a recent cybercrime, which was announced publicly as “The First Fraud of the Internet-of-Things” [30], the offenders attacked a network of ATMs used by financial institutions. Using web-based controls, the fraudsters caused the ATMs to ignore the balance of the compromised accounts. With the restriction removed, the fraudsters were able to extract $40 million from 12 accounts. This attack has demonstrated that the IoT lacks control of infrastructure and that even relatively low-level infrastructure can be used to cause significant damage. Moreover, most businesses currently turn to the IoT to manage multiple business processes. These interdependencies can increase the impact and damage caused by the compromised nodes and cause even more unintended consequences.

Copyright or intellectual property infringement. Two types of data exist in the IoT: 1) data that are created by the IoT end nodes such as sensors collecting data on their environments, 2) and data (content) that are transmitted through the IoT. Currently, existing copyright laws provide copyright protection only for the original artistic work, the author thereof is a natural person, excluding cinematographic works that can be produced by a corporation. There is a problem regarding the IoT where 'things' are capturing, communicating and exchanging information with other 'things' wirelessly. Much of the information being gathered by the IoT nodes may be very valuable. The end nodes of the IoT are able to collect or synthesize billions of bits of data and create valuable information that could not be created by a human author. As the IoT systems become even smarter, the IoT nodes will be operating not just as tools or sensors for collecting data, but also as producers of works with little human intervention. However, both in the US and Canada the copyright law does not cover "works produced by a machine or mere mechanical process that operates randomly or automatically without any creative input or intervention from a human author" [31]. However, as the demand for the data gathered by the IoT grows, a market for such data may arise in the future which may require for the change of copyright protection laws to protect the rights of the IoT system owners against public distribution of the IoT data even if does not contain any private information [31].

Malicious spamming. Recently Proofpoint, a cyber-security firm, became the first to report a global spam attack by a "thingbot" made up of 100,000 Internet-connected consumer gadgets that included home-networking routers, web-connected multi-media centers, televisions – and at least one refrigerator [32]. The attack has demonstrated that 'smart things' are poorly protected and consumers have no means to detect such malicious activity when it occurs. The IoT is a target-rich environment for cyber criminals, which is more attractive and easier to attack and control than PCs or tablets.

The cybercrimes in the IoT are summarized in Table 3.

Table 3. Crimes in the IoT

Sources	Devices	Cybercrime in the IoT
End nodes	Game consoles, mobile devices, smart TVs, tags, readers, embedded systems, home heating controllers, etc.	Distribution of malware (viruses), data theft, spamming, "thingbots"
Network	Wireless network routers, access points, sensor networks	Unauthorized access, data modification
Network perimeter devices	Servers, firewalls	Unauthorized access
Cloud	Cloud systems	Data theft
Web	Web clients, web servers, social networks	Fraud, Copyright or intellectual property infringement, cyber defamation, piracy

The implications of cybercrimes in the IoT

Actions that comprise a cyber-attack can be defined by their objectives as [22]: 1) capture; 2) disrupt, degrade, deny, destroy, and 3) manipulate.

Capture attacks, depending on the targeted resources, can focus on the attempt to gain control of physical or logical systems, while others can try to gain unauthorized access to information. Systems composing the IoT are uniquely susceptible to capture, due to a number of their characteristics. Their spatial distribution and ambient ubiquity give attackers excellent opportunities to gain physical or logical proximity to their targets. Increased mobility and interoperability increase the threat to the IoT systems by complicating access control and enabling an attacker to inject compromised systems into the IoT environment or remove the nodes in order to compromise and reintroduce them without any detection. Furthermore, heterogeneity of the IoT systems can complicate maintenance procedures to the point of increasing the window of vulnerability to a specific attack. Information in the IoT is widely distributed throughout the network, so that any successful capture of a system will likely result in capture of information to which that system has access.

Disrupt, degrade, deny, and destroy attacks are intended to disrupt the IoT systems. The combination of heterogeneity and interoperability in the IoT entities is a key factor to achieve resiliency. Heterogeneity is generally assumed to result in higher survivability for the network as a whole. In the event of disruption of one entity in the environment, other entities may resist the attack, and be able to continue functioning. The challenge is to verify integrity, confidentiality, and availability of all systems and data within the IoT environment.

Manipulation attacks are intended to influence opponents' decision cycles [33]. In the beginning, an attacker may manipulate the outside information itself. This involves intercession at the entry point in the information collection process, usually via physical means. Furthermore, an attacker may directly manipulate sensors that gather information. This same approach applies to the manipulation of controllers to change their actions, so that sensors observing the results of the controllers' actions would receive information that is not reflective of an undisturbed closed loop. Lastly, the attacker may manipulate the feed-forward mechanisms in the decision cycle, employing a man-in-the-middle or spoof attack. In this case, the attacker intercedes in communications between entities to exert control over the information transmission. Furthermore, each additional entity added to the network increases the number of possible intercommunications, and offers greater opportunity for an attack. Mobility and distribution in the IoT also increases an opportunity of the attack, as they make it easier to compromise the IoT systems without fear of detection.

Trends of a cybercrime

In recent years, a cybercrime has evolved towards a progressing disentanglement of a crime scene and crime act, growing criminal creativity and sophistication. As a result, the complexity of the cybercrime detection and analysis tasks will grow enormously, as the crime scene becomes globally diffused and the number of suspects may be huge.

Through the appearance and rise of social networks, the social dimension and societal impact of cybercrime has increased enormously. Projecting from current digital trends crime evolution into the future it is possible to highlight a few characteristics that will most probably define the face of a cybercrime for the years to come as follows: cybercrime becomes further socially networked and mobile; cybercrime becomes increasingly professional and industrialized; cybercrime means become easily accessible and adoptable by everyone.

The IoT and cyber-physical systems will outgrow current social web in the future. Cisco estimates that the IoT will grow from 15 billion connections in 2014 to over 50 billion in 2020, while the number of social network users will exceed 2 billion, and the number of mobile users will reach 9 billion (http://www.statista.com). Smart things and environments (such as smart home appliances, cyber-cars, and robots) will become the main provider and customers of various virtual services. Since, as per definition, they will be much less under direct control of human beings, their attractiveness and vulnerability for criminal activities will be very high. The number of criminal offences committed against critical IoT systems in government, companies, financial institutions, hospitals, etc. is likely to increase. This could lead to malware in critical systems leading to data loss, misuse or even killing of the critical systems [15].

INVESTIGATION METHODS OF CYBERCRIMES IN THE IoT

Digital forensics readiness and process

Forensic investigation is the use of science and technology to investigate and establish facts in criminal or civil courts of law [34]. The goal of any given forensic examination is to find facts, and to recreate the truth of an event via these facts. The examiner reveals the truth of an event by discovering and exposing the "footprints" or artefacts of the illegal action on the system [35]. Digital forensics denotes the forensic process of employing scientific principles and processes to analyse electronically stored information in order to determine the sequence of events, which lead to a particular incident [36]. Noblett *et al.* [37] define computer evidence as: 1) physical items such as chips, boards, central processing units, storage media, monitors, and printers that can be described as a unique form of physical evidence; and 2) information items such as logging, description, storage, and disposition that can be described easily and correctly as a unique form of informational evidence.

The challenge to computer forensic science is to develop methods and techniques that provide valid and reliable results while protecting the real evidence—the information—from harm [37]. Electronic information is fundamental to the successful handling of such incidents. If an organization does not prepare proactively for such incidents, it is highly likely that important relevant digital evidence will not be available. Tan [38] defines the forensic readiness as having two objectives: 1) maximizing an environment's ability to collect credible digital evidence, and 2) minimizing the cost of forensics during an incident response. Rowlingson [39] refines these goals as follows: 1) to gather evidence legally and without interfering with business processes; 2) to gather evidence targeting the potential crimes; 3) to allow an investigation to proceed at a cost in proportion to the incident; 4) to minimize interruption of business processes from an investigation;

If an organization establishes the digital forensics readiness program, it can apply a digital forensics process to respond to security incident. There are multiple digital forensic investigation methods defined to date to identify the digital forensic process [40-45]. Kohn *et al.* [46] have defined six the most diverse and the most comprehensively represented digital forensics process models (DFPMs) that consist of the following sequential phases: 1) preparation; 2) incident, incident response; 3) digital forensic investigation; 4) presentation. In addition, a *documentation* process, which is executed in parallel to every process, is included.

Digital Forensics Management in the context of the IoT

The IoT poses some challenges for forensics investigators including the widened spread of data and information, the blurring of lines between networks, and the expectation of privacy by users with personal networks increasingly fading into non-personal ones and private networks blurring into public ones. A number of factors that should be considered when an IoT-related crime scene is approached (Table 4). One of such factors is the kind of hardware evidence involved. The IoT is envisaged as a system that involves communication between wide varieties of objects from devices that already communicate (networked PCs, mobile phones, etc.) to the devices that will be enabled to communicate (household appliances, etc.).

Table 4. Differences between the traditional and IoT digital forensics investigations

Criterion	**Traditional**	**IoT**
Speed of response to incident	Typically after the incident	This is too slow for the IoT.
Variety of evidence sources and types	Wide measurable range	Even wider range
Frameworks adaptable	Possibly	Absolutely crucial
User input	User is either perpetrator or the victim – does not play role in the investigation	User must be enabled to keep personal IoT under forensic surveillance by the use of adaptable, commercially available forensic solution.
Evidence Sources	PC, Cloud, virtualization, mobile communication devices, web clients, social networks, Authentication Authorisation and Accounting (AAA) servers, gateways e. g. proxy servers.	Home appliances, cars, tags, readers, embedded systems sensor nodes, sensor networks, medical implants in humans and animals, other IoTware.
Jurisdiction	Individual, social networks, society, Company, government	Same
Number of devices	Billions of devices	50 billion by 2020 to trillions of devices
Types of evidence	Electronic documents, standard files formats e. g. jpeg, mp3 etc.	Any and all formats possible.
Types of networks	Wired, Bluetooth networks, mobile communications, Wi-Fi, wireless internet,	RFID, sensor networks, e. g. sensor to reader and vice versa.
Quantity and type of data and evidence	Up to terabytes of data	Up to Exabyte of data.
Protocols	Ethernet, wireless (802. 11 a,b,g,n), Bluetooth, IPv4 and IPv6	RFID, Rime (14).
What to seize	Seize devices as required	Identify possible Next Best Things for source of evidence
Ownership	Individuals, groups, companies, governments, etc.	Same
Network boundaries	Relatively clearly-defined boundaries and lines of ownership	Increasingly blurry boundary lines

Characteristics of digital evidence

Digital evidence refers to any electronic digital data that are sufficient to prove the circumstances or the association of a crime in a computer environment [36]. Wang provides a similar definition that digital evidence is any data that can provide a significant link between the perpetrator and the victim [47]. Physical characteristics of the digital evidence are as follows [36]:

1. It is easily copied and modified, but not easily retained in its original state. Confirmation of the original digital source is, therefore, susceptible to doubt.
2. Its source and integrity are not easy to prove. This makes it very difficult to directly infer the relationship between the evidence obtained and the suspects and to guarantee that the evidence has not been changed.
3. The presentation of digital information cannot be well perceived by human senses without the help of a suitable toolkit.
4. There are innumerable sources of potential digital evidence. The list is summarized in Table 5 (based on [48]).

Table 5. Potential sources of evidence

Source	Description
Access control logs	Usually access control systems can be configured to maintain records of when usernames and passwords were issued, when passwords were changed, when access rights were changed and/or terminated. In addition, many systems also maintain logs of failed accesses.
Anti-virus logs	These logs record the detection and destruction of viruses and worms. A common defence tactic is to suggest that suspicious behaviour has been caused by a rogue program; anti-virus logs often contribute to resolving such claims.
Back-up media	Some organizations back up their entire systems every 24 hours; others have in place a partial, incremental policy. Back-up archives are extremely important sources of evidence, as they can show if “live” files have been tampered with. They can also provide data which has been deleted from the “live” system.
CCTV recordings	Until recently CCTV material was stored on tapes in analogue format. But the cost of digital storage – to fast hard-disk – has plummeted. Digital storage means that CCTV images can be rapidly identified by date and time of incident. In addition motion detection and other analytic software can be deployed. At the same time the cost of cameras has collapsed as well, so that many more locations can be made the subject of surveillance
Configuration, event, error and other internal files and logs	All computers contain files which help to define how the operating system and various individual programs are supposed to work. Often, there are important configuration files associated with individual programs. Many operating systems also generate error and other internal logs.
Email traffic	Emails potentially provide important evidence of formal and informal contacts.
Internet activity logs	Individual PCs maintain records of recent web access in the form of the history file and the cache held in the temporary internet files folder. But many corporate networks also maintain centralised logs, if only to test quality of service and check against abuse. These logs should be properly managed and preserved, then they are powerful evidence of activity.
Intrusion detection logs	Larger computer systems often use intrusion detection systems as part of their security measures – they are intended to detect and prevent several forms of hacking. Producing such logs may help to identify perpetrators, or demonstrate that reasonable precautions have been taken to secure the system.
Main business and transaction records	These include all purchases, sales and other contractual arrangements at the heart of the business.
Records held by third parties	Where an organization has out-sourced some of its key functions to a specialist ICT business or cloud computing provider, records may not be under its immediate direct control.
Selected data media	Most computer users archive all or part of their activities on external storage media. These include CD-ROMs, Digital Versatile Discs (DVDs), floppy disks, tape, external hard disks, memory cards and Universal Serial Bus (USB) thumb drives. There needs to be a routine for identifying all of these and securing them, pending examination.
Selected individual personal computers (PCs)	If individuals are under any form of suspicion, the organization will need to be able to seize their PCs and make a proper forensic “image”, which produces a precise snapshot of everything on the hard disks (this includes deleted material which technicians may be able to recover).

Source	Description
Selected mobile phones / smart phones/ tablets/PDAs etc.	These devices can hold substantial amounts of data. Technical methods for preserving and investigating them are more complex than those for PCs; in addition there may be additional legal problems as ownership and privacy rights may not be wholly clear.
Social networking	Social networks are quickly becoming what instant messengers were just a few years ago. More and more communication is migrating from public chat rooms and private messengers into online social networks.

Techniques of the analysis of digital evidence

Once the appropriate digital evidence has been collected, and since the digital evidence comes in big quantities, it is extremely important that some sort of initial prioritization be undertaken. This process is called triage [49]. If prioritizing of digital evidence is executed using information obtained from automatic tools, the term "digital triage" is used [50, 51]. The goal of digital triage is to produce intelligence rather than legal evidence. Once the digital evidence is prioritized, the analysis techniques of the collected digital information are divided into two groups under categories of the collected data: 1) live analysis; and 2) static or dead analysis or post-mortem.

Live analysis is usually performed on volatile data [52], meanwhile the static analysis is performed on permanent data storage. One of the main aims of live forensics is to collect and analyse volatile memory data. Most live forensic approaches focus on analysing a single snapshot of a memory dump [52]. The search, data mining, event reconstruction and timestamp analysis techniques can be used to search for collected persistent information.

Search techniques. According to the level of the search automation, search techniques can be classified into manual browsing and automated searches [53]. Manual browsing is used to browse collected information and look for the desired objects. A viewer of some sort is the only tool used in the process. Forensic investigations usually collect large amounts of digital information, which makes manual browsing of the entire collected dataset unacceptably long. However, manual browsing is still required to browse the selected pieces of data. Automated searches include keyword search, regular expression search, and approximate matching search. Keyword search is an automatic search of information for data objects containing specified key words. However, in order to specify the desired type of data objects precisely, keywords are rarely sufficient. Regular expressions provide a more flexible language for describing the objects of interest than keywords. However, regular expression searches suffer from false positives and false negatives just like keyword searches, because not all types of data can be adequately defined using regular expressions. Approximate matching search uses matching algorithm that permits character mismatches when searching for a keyword or pattern.

Data mining techniques. Due to exponential growth of data storage, larger corporations and law enforcement agencies face digital investigations with terabyte-sized datasets [54]. Processing times for the limited keyword searches can take days, and the analyst may be overwhelmed with the number of hits to review. Consequently, search techniques cannot be used efficiently on large data sets. Data mining techniques can be used to solve this problem [55]. Data mining processes, methods and techniques can be divided into three major classes: descriptive modelling [56], predictive modelling [57], and content retrieval [58]. Descriptive modelling summarizes data, whereas predictive modelling identifies characteristics that allow to predict future observations. Content retrieval data mining extracts information from complex and/or semi-structured/unstructured data sets.

Event reconstruction techniques. The reconstruction of events in a computer requires thorough understanding of the computer architecture and functionality, which is directly related to the operating system of the computer. Log file entries are generated by system processes when something important in a system happens. These entries allow the forensic analyst to infer specific knowledge about certain events that have happened.

Timestamp analysis. Timestamps are important in digital investigations, since they are necessary for the association of evidence from different sources, particularly for the event reconstruction. The main problem is that the use of timestamps as evidence can be questionable due to the reference to a clock with unknown adjustment. Willassen [59] proposed to create a system model by listing all possible timestamping orders, and determining, which timestamping orders are possible in the system and which action sequences may cause them. From the list of possible and impossible timestamping orders, invariants for a system can be derived. These invariants can be used to test a hypothesis for the consistency with evidence stored on an investigated system. Thus, the real time of stamping can be established, which can be used to correlate the time of the events on a digital system with events occurring elsewhere.

The analysis of digital evidence in the IoT

The IoT is designed as a network of smart, decision-making, self-managing systems and services [60]. There are few scientific publications on the forensics of the digital evidence in the IoT. However, based on the composition of structural parts of the IoT one can analyse and by analogy apply the forensics techniques from the related domains such as: smartphones, wireless computer networks, and cloud services. Various major areas make up the IoT. These areas include Cloud, virtualisation, mobile devices, fixed computing, sensor and RFID technologies. Forensics in the IoT will, therefore, encompass forensics in all these areas and more. However, the boundaries of networks and devices is increasingly blurry in the IoT forensics.

Digital evidence in smartphones

Smartphones structurally can be end nodes in the IoT. Parts of smartphones (such as sensors, microcontrollers) can also be parts of the IoT. Consumerization of smartphones has triggered the forensic community to focus on technical details of these devices as well as data acquisition in: (a) Windows Mobile [61, 62], (b) Symbian [63, 64], (c) iOS [65, 66], and (d) Android [67, 68]. Moreover, Mobile Device Forensics (MF) can be applied to a wide range of computing devices rather than mobile phones only. In order to associate smartphone data to evidence types, smartphone data can be categorized according to their source [69]: messaging data, i.e. the content and metadata (e.g. sender, delivery time, etc.) from messaging services (e.g. Short Message Service (SMS), e-mail etc.); device data, i.e. data that are stored in the device storage media and are not related to any application (e.g. multimedia files, software and hardware identifiers, etc.); (U)SIM Card Data that reside in a (Universal) Subscriber Identity Module, such as IMSI2 and MSIN3; usage history data, i.e. user logs (e.g. call logs, browsing history, etc.) and system logs kept for monitoring and debugging; application data, i.e. permanent or temporal data that are used during application execution (e.g. flat files, databases, etc.); sensor data, which are created by sensors that are found in most devices (e.g. camera, microphone, global positioning system (GPS), motion sensors (accelerometer, gyroscope), or environment sensors (magnetometer, proximity, light, temperature, etc.); user input data, i.e. data from keystrokes, which are processed on the fly, or stored in a keyboard cache.

The widespread use of smartphones introduces new opportunities as well as challenges in digital forensics. Smartphones are usually equipped with sensors, hardware which can be used to infer user's context. This context may be useful in a digital investigation, as it can help to reject or accept an alibi, or even reveal a suspect's actions. However, the majority of sensor data, which are volatile and time sensitive, cannot be collected during a post-mortem investigation. Therefore, time stamped evidence derived from sensor data can hardly be found on the device after a crime has been committed, unless they have been explicitly collected. GPS-enabled devices may contain remnants of past locations and maps that can be useful in an investigation. Some mobile devices record the location of cellular towers they contacted, providing a historical record of the user's location. In addition, the EXIF data embedded in digital photographs can provide the date and time the photograph was created, the device type used to create it, and potentially the GPS coordinates of the location the photograph was taken.

Since the majority of sensor data are volatile, they are not available in the post-mortem analysis. Therefore, the only way to timely acquire them, in case such a need arises during a digital investigation, is by software that collects them when they are generated by the suspect's actions. Mylonas *et al.* [70] examine the feasibility of ad-hoc data acquisition from the smartphone sensors by implementing a device agent for their collection in Android, as well as a protocol for their transfer. However, a smart phone is a personal belonging, information of which stored inside, is protected by the right to privacy. The forensic investigator should take extra caution, when investigating the use of the smart phone as the tool of a cybercrime [71].

There are three standard ways to get forensic information from smartphones: manual, logical and physical analysis (Table 6). Each one uses different attributes of the device for extracting the desired amount of data [72]. Manual acquisition is defined as interacting with installed applications in the device itself to copy the existing data. Logical acquisition retrieves a bitwise copy of the information in a logical storage of the target mobile device and provides context information such as date-time stamps and location within the file system [36]. It mainly concerns data that have not been deleted. Data that have already been deleted are less likely to be acquired. Physical acquisition is solely related to the physical storage medium and includes, e.g., retrieval of deleted files, which is treated as unallocated but still exists in memory; or bypassing user security mechanisms such as passwords and screen locks.

Table 6. Methods of extracting information from mobile devices

Method	Description
Manual operation via user interface	Examiner manually accesses the phone through the user interface. Only data accessible through the operating system is retrievable.
Logical acquisition via communication port	Logical acquisition methods interact with mobile devices using protocols such as AT commands and OBEX (OBject Exchange), and only extract data that are accessible through the OS.
Physical acquisition via communication port or proprietary interface	Extracts the memory contents in their entirety through the communications port. Interpreting the extracted binary is dependent on understanding how the phone stores data in memory structures.
Physical acquisition via JTAG	Uses the JTAG interface to extract the memory contents of the device. It allows the extraction of full binaries. Acquiring digital evidence via the JTAG is less intrusive than relying on the device operating system, but interpreting the extracted binary requires in-depth knowledge of the device.
Physical acquisition via direct memory chip access	The lowest-level and potentially most complex acquisition method for mobile devices. Involves extracting memory chips from the device and reading the memory structures. It can provide access to all device content, but requires knowledge of interpreting the raw structures. This technique should not be used for cases when the original device must remain operable.

Standard digital evidence extraction methods are as follows: data extracted using common PC-to-device communication protocols: AT, OBEX, SyncML; Smartphone connected to PC with a standard cable (or Bluetooth/IR adapter); data extracted using direct memory reading (hex dump); embedded device (or its memory chip only) connected to special hardware techniques like Joint Test Action Group (JTAG) [73] to extract data from the device or use an (adapted) bootloader to gain low level of access to the device.

The Object Exchange Protocol (OBEX) technology for Windows Mobile provides an efficient, compact binary protocol that enables a wide range of devices to exchange data spontaneously in a simple, efficient manner. This technology works over Bluetooth and Infrared Data Association (IrDA) protocols. OBEX requires little resources and could be used for low-end devices.

The JTAG port is generally used by manufacturers for testing circuit boards [73]. However, the port can also be used to forensically acquire data and/or an image from a specific embedded system. It is a standard feature found in many mobile phones, as it provides manufacturers a low-level interface to the device that is not dependent on the operating system. However, the JTAG specifications for individual phones are not available outside the manufacturer. JTAG is of interest to forensic investigators and analysts, as it can theoretically provide direct access to a mobile phone’s memory without any chance of altering it.

Digital evidence in wireless computer network devices

The same digital evidence gathering techniques as in wireless computer networks can also be applied to Wireless Sensor Networks (WSN). However, collecting a complete set of data from network sources require an approach different from traditional storage media forensics. This is a huge challenge if the network has unpredictable communication channels like wireless ad hoc networks [74]. Digital forensics of the IoT will have to take into account the movement of people, with their IoT devices and services, between networks. Network forensics would typically follow the systematic process of [75]: closing the network ports or processes that allowed the intruder to carry out the attack; acquiring the drive which had been compromised; making an exact replica of the drive with a bit-stream image; and verification the duplicate image to the original image.

A network is set up using a router, a networking device that forwards data packets between computers and other devices such as sensors. A wireless access point would be the most interesting for potential evidence, as a certain level of information that can be provided by such devices, including the SSID, the encryption and type of a key, DHCP status, the information related to MAC address filtering, and operating system data [76].

Digital evidence in cloud services

Cloud forensics will play a key role in the sphere of the IoT forensics especially since the data generated from the IoT networks and services are already, or will increasingly be stored, on cloud locations [60]. Cloud computing-based services and, specifically, cloud enabled storage services have become an increasingly important part of the IoT infrastructure. As with the most new technologies cloud storage services have the capacity to be used for criminal exploitation.

Therefore, features synonymous with cloud (storage) services such as multi-tenancy, data security, file encryption and communications encryption also need to be addressed as a part of a digital forensics investigation [77].

Digital forensics in cloud follows the common cybercrime forensics scheme as follows [78]: 1. evidence source identification and preservation: identifying sources of evidence in a digital forensics investigation. 2. collection: actual capture of the data. 3. examination and analysis: examination and analysis of forensic data. 4. reporting and presentation: legal presentation of the evidence collected.

The large quantities of data generated by the IoT and stored in large-scale distributed cloud environments are the subject of a cloud investigation. However, there are a number of technical barriers; the IoT data is either stored on proprietary devices that are difficult to interface with or in cloud computing platforms where the scale, distribution and remote nature of the data preclude imaging as a viable extraction process. Distributed analysis techniques are required to analyse the data stored in cloud computing platforms [79]. In case of cloud computing, digital forensics should be performed both on client and server side. On the client side, common sources of evidence in case of digital forensics research of cloud-based services are: sync and file management metadata and configuration data stored to facilitate the sync process between client and server can be useful in identifying the available evidence for collection from the server environment and used to build a file management history; cached files – the files the user has stored on the client device and uploaded to the cloud environment or downloaded from the cloud environment to the client device; cloud service and authentication data – commonly consist of an address (DNS, IP, URL, etc.) and potentially stored credentials of the user; encryption metadata – they could include databases/configurations detailing which files are encrypted and using which algorithm, keys, etc.; browser artefacts – these may also include file metadata often found in URLs.

On the server side, common sources of evidence in case of digital forensics research of cloud-based services are: administrative and file management metadata, which store the configuration of the cloud instance and of individual users within the cloud instance as well as database and configuration files which list the files and data stored by the user on the cloud instance; stored files – the data uploaded by the user to the cloud instance; encryption metadata – data relating to encryption (if enabled) in the cloud instance, specifically data relating to decrypt the user data; cloud logging and authentication data – data associated with transactions made by the user with the cloud instance (files uploaded/downloaded, login events, etc.).

The summary of forensics evidence in IoT is provided in Table 7.

Table 7. Potential sources of evidence in the IoT

Sources	**Devices**	**Evidences**
End nodes	Game consoles, mobile devices, smart TVs, tags, readers, embedded systems, home heating controllers, etc.	Sensor data, IP address
Network	Wireless network routers, access points, sensor networks	Logs
Network perimeter devices	Servers, firewalls	Network and system logs, authentication data, etc.
Cloud	Cloud systems	Client virtual machines; logs
Web	Web clients, web servers, social networks	Web logs, user activity

CONCLUSIONS

The Internet of Things (IoT) defines a worldwide cyber-physical system that connects all types of physical objects over the Internet and has a plethora of applications in the fields of domestics, e-health, goods monitoring and logistics, dissemination of digital content, among others. The IoT is inherently complex. The vast size, ubiquity and physical distribution of it makes the task of defending it against cybercrime threats and attacks unachievable. The limitations of the IoT (such as the requirements for low power) further contribute to the problem by prohibiting the use of high-security but resource-greedy cryptography techniques. The IoT will become the platform for the cybercrimes. Attackers will continue to take the advantage of the low levels of understanding of the IoT technologies and safety practices to defraud people and organizations. As the number of existing and future threats and attacks is only going to increase in both intensity and severity, new approaches to digital forensics IoT systems are required.

The appearance and rise of social networks resulted in great growth of the social dimension and societal impact of a cybercrime. As new devices and new technologies constantly emerge, the IoT presents many new challenges to digital forensics investigations. The IoT possesses vast quantities of data. In addition to being voluminous, web data is exceptionally "noisy" regarding the investigative objectives. The sheer volume and "noisiness" of these data, the heterogeneous nature of the IoT devices, the ways in which data are distributed, aggregated, and processed require the development of new methods of the digital forensics investigation. The analysis of operations and application models of the IoT, traditional cybercrime forensics methods and tools indicates that in order to investigate a cybercrime on the IoT new, innovative digital forensics readiness and investigation methods are needed to be developed.

ACKNOWLEDGEMENTS

The investigation presented in this paper has been carried out partially within the project "Lithuanian Cybercrime Centre of Excellence for Training, Research and Education", Grant Agreement No HOME/2013/ISEC/AG/INT/4000005176, co-funded by the Prevention of and Fight against Crime Programme of the European Union.

REFERENCES

[1] C. Han, J. M. Jornet, E. Fadel, I. F. Akyildiz. A cross-layer communication module for the Internet of Things. Computer Networks 57 (2013) 622–633.

[2] K. H. Johansson, G. J. Pappas, P. Tabuada, C. J. Tomlin. Guest Editorial: Special Issue on Control of Cyber-Physical Systems. IEEE Transactions on Automatic Control, Vol. 59, No. 12, 3120-3121, 2014.

[3] Evans D. The Internet of Things. How the Next Evolution of the Internet Is Changing Everything. (2011) http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (Accessed 2014. 11. 06)

[4] Sundmaeker, H., P. Guillemin, P. Friess, S. Woelfflé (Eds.). Vision and challenges for realising the Internet of things. Luxembourg, 2010, 229 p.

[5] Marias, G. F., Barros, J., Fiedler, M., Fischer, A., Hauff, H., Herkenhoener, R., Grillo, A., Lentini, A., Lima, L., Lorentzen, C., Mazurczyk, W., de Meer, H., Oliveira, P. F., Polyzos, G. C., Pujol, E., Szczypiorski, K., Vilela, J. P. and Vinhoza, T. T. V. (2012), Security and privacy issues for the network of the future. Security Comm. Networks, 5: 987–1005. doi: 10.1002/sec.384

[6] Liebrand K. et all. (2011) Ethics, Privacy and Data Protection in BUTLER. http://www.iot-butler.eu/wp-content/plugins/download-monitor/download. php?id=24 (Accessed 2014. 10. 24)

[7] Nieto A., and Lopez J. (2014), Analysis and taxonomy of security/QoS tradeoff solutions for the future internet, Security Comm. Networks, 7, 2778–2803, doi: 10.1002/sec.809

[8] J. Sutanto, E. Palme, C. -H. Tan, and C. W. Phang. Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. MIS Quaterly, 37(4), 1141-1164 (2013)

[9] T. Heer, O. Garcia-Morchon, R. Hummen, S.L. Keoh, S.S. Kumar, and K. Wehrle. Security Challenges in the IP-based Internet of Things. Wireless Personal Communications 61 (3), 527-542.

[10] Newman, G. R. Cybercrime, In Krohn M. D., Lizotte A. J., and Hall G. P. (Eds.). Handbook on Crime and Deviance, Criminology and Criminal Justice Series, Springer Science, 2009, pp. 551-584.

[11] Marion, N. E. The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation. International Journal of Cyber Criminology, Vol. 4 Issue 1&2 January - July 2010 / July - December 2010, 699–712.

[12] United Nations. The United Nations manual on the prevention and control of computer related crime, supra note 41, paragraphs 20 to 73 in International Review of Criminal Policy, pp. 43–44 (1995)

[13] Gordon S., and Ford R. On the definition and classification of cybercrime. Journal in Computer Virology, Volume 2, Number 1, August 2006, 13-20.

[14] ITU (International Telecommunication Union). The Internet of Things. ITU Report, Nov. 2005.

[15] Saini H., Rao Y. S., and Panda T. C. International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 2,Mar-Apr 2012, pp. 202-209.

[16] Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J. and Deng, H. (2012), A survey of cyber crimes. Security Comm. Networks, 5: 422–437. doi: 10.1002/sec.33

[17] Helfenstein S., and Saariluoma P. How cyber breeds crime and criminals. In V. Snasel (Ed.), DigitalSec 2014 Proceedings: The International Conference on Digital Security and Forensics (pp. 76-90). Wilmington: The Society of Digital Information and Wireless Communications (SDIWC).

[18] Felson, M. and Clarke, R. V. Opportunity Makes the Thief: Practical Theory for Crime Prevention. Police Research Series, Paper 98, 1998, Home Office, London.

[19] Loch K. D., Carr H. H., and Warkentin, M. E. Threats to information systems: today's reality, yesterday's understanding, MIS Quarterly, vol. 16, iss. 2, 2012, 173-185.

[20] Mayer C. P. Security and privacy challenges in the internet of things, Electronic Communications of the EASST, vol. 17, 2009.

[21] Babar S., Mahalle P., Stango A., Prasad N. R., and Prasad R. Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT). CNSA 2010: 420-429.

[22] Covington, M. J., and Carskadden, R. Threat Implications of the Internet of Things. 5th International Conference on Cyber Conflict (2013): 1-12. IEEE.

[23] Mayrhofer, R. (2014), An architecture for secure mobile devices. Security Comm. Networks. doi: 10.1002/sec.1028

[24] Garcia-Morchon, O., Kumar, S. Security Considerations in the IP-based Internet of Things, Sept. 11., 2013. http://tools.ietf.org/html/draft-garcia-core-security-06 Accessed October 24, 2014

[25] Shipley, A. J., Security in the Internet of Things. Wind River, Sept. 2013. http://www. windriver. com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internetof-things. pdf Accessed October 24, 2014

[26] Gamer, T., Völker, L. and Zitterbart, M. (2011), Differentiated security in wireless mesh networks. Security Comm. Networks, 4: 257–266. doi: 10.1002/sec.163

[27] Suo H., Wan J., Zou C., and Liu J. Security in the Internet of Things: A Review. Proc. of the 2012 Int. Conference on Computer Science and Electronics Engineering – Vol. 03 (ICCSEE '12), Vol. 3, 648-651.

[28] Li Z., and Xin T. Threat Modeling and Countermeasures Study for the Internet of Things, JCIT. Papers 8(5), 1163 - 1171(2013).

[29] Tsao T., and Alexander R. Security Threat Analysis for Routing Protocol for Low-power and lossy networks (RPL), Dec. 15, 2013. http://tools.ietf.org/pdf/draft-ietf-roll-security-threats-06.pdf. Accessed October 24, 2014

[30] Katz E. The First Fraud of the Internet-of-Things (IoT), April 30, 2014 http://insights.wired.com/profiles/blogs/the-first-fraud-of-the-internet-of-things-iot Accessed October 24, 2014.

[31] Abe-Oldenburg L. K. The Internet of Things and Canadian Copyright Law. http://blog.bennettjones.com/2014/09/23/internet-things-canadian-copyright-law/ Accessed October 24, 2014.

[32] Proofpoint. Proofpoint Uncovers Internet of Things (IoT) Cyberattack. January 16, 2014. http://www.proofpoint.com/about-us/press-releases/01162014.php

[33] Applegate S. D. The Principle of Maneuver in Cyber Operations, in 2012 4th International Conference on Cyber Conflict, vol. 4, Talinn, Estonia, 2012, p. 13.

[34] Philipp, A., Cowen, D., and Davis, C. Hacking Exposed Computer Forensics. McGraw-Hill, 2nd edition, 2009, 650 pp.

[35] Altheide, C., Carvey, H. Computer and Intrusion Forensics. 2003, ARTECH HOUSE, INC., 685 Canton Street Norwood, MA 02062, USA.

[36] Casey, E. Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet, 3rd edition, Academic Press, 2011, p. 807.

[37] Noblett, M. G., Politt, M. M, Presley, L. A. Recovering and Examining Computer Forensic Evidence. Forensic Science Copmmunications. October 2000, Volume 2, No. 4, http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm/#Top%20of%20article (Accessed 2014. 10. 25)

[38] Tan, J. Forensic readiness.http://isis.poly.edu/kulesh/forensics/forensic_readiness.pdf. July 2001. Accessed 2014-10-23.

[39] Rowlingson, R. A Ten Step Process for Forensic Readiness. International Journal of Digital Evidence, Vol. 2, Iss. 3, pp. 1-28, 2004.

[40] Palmer, G. L. Forensic analysis in the digital world. International Journal of Digital Evidence, Spring 2002, Vol. 1, Iss. 1, pp. 1–6.

[41] Reith, M., Carr, C., Gunsch, G. An examination of digital forensic models. International Journal of Digital Evidence, Vol. 1, Iss. 3, Fall 2002, pp. 1–12.

[42] Carrier, B. and Spafford, E. Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence, Vol 2, Iss. 2, 2003, pp. 1-20.

[43] Mandia, K., Prosise, C., Pepe, M. Incident response & computer forensics. 2nd edition, McGraw-Hill/Osborne, Emeryville, 2003, p. 507.

[44] Ó Ciardhuáin S. An extended model of cybercrime investigations. International Journal of Digital Evidence, Vol. 3, Iss. 1, Summer 2004, pp. 1–22.

[45] Beebe, N. L., Clark, J. G. A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation. Vol. 2, Iss. 2, June 2005, pp. 147–167.

[46] Kohn, M. D., Eloff, M. M., Eloff J. H. P. Integrated digital forensic process model. Computers & Security, Vol. 38, 2013, pp. 103-115.

[47] Wang, S. -J. Measures of Retaining Digital Evidence to Prosecute Computer-Based Cyber-Crimes. Computer Standards & Interfaces, 2007, 29 (2), pp. 216-223.

[48] Sommer, P. Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers. Fourth Edition, November 2013.

[49] Cantrell, G., Dampier, D., Dandass, Y., S., Niu, N., Bogen, C. Research toward a Partially-Automated, and Crime Specific Digital Triage Process Model. Computer and Information Science Vol. 5, No. 2, March 2012, pp. 29-38.

[50] Hong, I., Yu, H., Lee, S., Lee, K. A new triage model conforming to the needs of selective search and seizure of electronic evidence. Digital Investigation, Vol. 10, Issue 2, 2013, pp. 175-192.

[51] Horsman, G., Laing, C., Vickers, P. A case-based reasoning method for locating evidence during digital forensic device triage. Decision Support Systems, Vol. 61, 2014, pp. 69-78.

[52] Law, F. Y. W., Chan, P., Yiu, S., Tang, B., Lai, P. K. Y., Chow, K., Ieong, R. S. C., Kwan, M. Y. K., Hon, W., Hui, L. C. K.: Identifying Volatile Data from Multiple Memory Dumps in Live Forensics. In IFIP Int. Conf. Digital Forensics, 2010, pp. 185-194.

[53] James, J. I., Gladyshev, P. A survey of digital forensic investigator decision processes and measurement of decisions based on enhanced preview. Digital Investigation. Vol. 10, No. 2, 2013, pp. 148-157.

[54] Sommer P. The challenges of large computer evidence cases. Digital Investigation, vol. 1, 2004 pp. 16-17.

[55] Han, J., and Kamber, M. Data Mining: Concepts and Techniques, Academic Press, San Diego, California, 2001, 550 p.

[56] Al-Zaidy, R., Fung, B. C. M. ; Youssef, A. M., Fortin, F. Mining criminal networks from unstructured text documents. Digital Investigation, vol. 8, iss. 3-4, 2012,pp. 147-160.

[57] Dagher, G. G., Fung, B. C. M. Subject-based semantic document clustering for digital forensic investigations. DATA & KNOWLEDGE ENGINEERING, vol. 86,, JUL 2013,pp. 224-241.

[58] Ko, S.-J. A Text Mining-based Intrusion Log Recommendation in Digital Forensics. KIPS Transactions on Computer and Communication Systems, Volume 2, Issue 6,2013, pp. 265-276.

[59] Willassen S. Y. Timestamp evidence correlation by model based clock hypothesis testing. Proc. of the 1st int. conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop, 2008, Article No 15.

[60] Oriwoh, E., Jazani, D., Epiphaniou, G., Sant, P. Internet of Things Forensics: Challenges and approaches. 9th Int. Conference Conference on Collaborative Computing: Networking, Applications and Worksharing, 20-23 Oct. 2013, pp. 608-615.

[61] Casey E, Bann M, Doyle J. Introduction to windows mobile forensics. Digital Investigation 2010; 6(34), pp. 136-146.

[62] Grispos, G., Storer, T., Glisson, W. B. A comparison of forensic evidence recovery techniques for a windows mobile smart phone. Digital Investigation 2011;8(1), pp. 23-36.

[63] Distefano A, Me G. An overall assessment of mobile internal acquisition tool. Digital Investigation 2008;5, Supplement, pp. 121-127.

[64] Pooters I. Full user data acquisition from Symbian smart phones. Digital Investigation 2010;6(34), pp. 125-135.

[65] Bader, M, Baggili, I. iPhone 3GS forensics: Logical analysis using apple iTunes backup utility. Small Scale Digital Device Forensics Journal 2010; 4(1), pp. 1-6.

[66] Zdziarski, J. Identifying back doors, attack points, and surveillance mechanisms in iOS devices. Digital Investigation, Vol. 11, No. 1. (March 2014), pp. 3-19.

[67] Vidas, T., Zhang, C., Christin, N. Toward a general collection methodology for Android devices, Digital Investigation 8, August 2011, p. S14-S24.

[68] Mutawa N, Baggili I, Marrington A. Forensic analysis of social networking applications on mobile devices. Digital Investigation 2012;9, Supplement, pp. S24-33.

[69] Mylonas A, Meletiadis V, Tsoumas B, Mitrou L, Gritzalis D. Smartphone forensics: A proactive investigation scheme for evidence acquisition. Gritzalis D, et al., editors, Proc. of the 27th IFIP International Information Security and Privacy Conference. Springer; AICT-376; 2012. p. 249–60.

[70] Mylonas A., Meletiadis V., Mitrou L, Gritzalis D., Smartphone sensor data as digital evidence, Computers and Security, 38, October, 2013, pp. 51-75.

[71] Chang, C. -P., Chen, C. -T., Lu, T. -H., Lin, I. -L., Po, H., Lu H. -S. Study on Constructing Forensic Procedure of Digital Evidence on Smart Handheld Device. Proceedings of IEEE International Conference on System Science and Engineering, July 4-6, 2013, pp. 223-228.

[72] Barmpatsalou, K., Damopoulos, D., Kambourakis, G., and Katos, V. A critical review of 7 years of Mobile Device Forensics. Digit. Investig. 10, 4 December 2013, pp. 323-349.

[73] Breeuwsma IM. Forensic imaging of embedded systems using {JTAG} (boundary-scan). Digit Investig., 3(1), 2006, pp. 32–42.

[74] Mutanga, M. B. ; Mudali, P. ; Dlamini, IZ. ; Ndlovu, L. ; Xulu, S. S. ; Adigun, M. O. Challenges of evidence acquisition in wireless ad-hoc networks, IST-Africa, 2010, pp. 1-8.

[75] Szewczyk, P. ADSL Router Forensics Part 1: An introduction to a new source of electronic evidence. Proc. of the 5th Australian Digital Forensics

Conference, Edith Cowan University, Perth Western Australia, 2007, pp. 1-6.

[76] Turnbull, B. ; Slay, J., Wi-Fi Network Signals as a Source of Digital Evidence: Wireless Network Forensics, Third International Conference on Availability, Reliability and Security, 2008. ARES 08,4-7 March 2008, pp. 1355-1360.

[77] Chung H, Park J, Lee S, Kang C. Digital forensic investigation of cloud storage services. Digital Investigation. 9(2), 2012, pp. 81–95.

[78] Martini, B., and Choo K. -K., R., 2013. Cloud storage forensics: ownCloud as a case study. Digit. Investig. 10, 4, (December 2013, pp. 287-299.

[79] Hegarty, R. C., Lamb, D. J., and Attwood, A. Digital Evidence Challenges in the Internet of Things. Proc. of the 9th Int. Workshop on Digital Forensics and Incident Analysis, 2013, pp. 163-172.