The Forensic Swing of Things

"The current legal and technical challenges of IoT Forensics"

Pantaleon Lutta, Mohamed Sedky, Mohamed Hassan

Abstract**—**The inability of organizations to put in place management control measures for Internet of Things (IoT) complexities persists to be a risk concern. Policy makers have been left to scamper in finding measures to combat these security and privacy concerns. IoT forensics is a cumbersome process as there is no standardization of the IoT products, no or limited historical data is stored on the devices and them being always connected makes them extremely volatile. This paper highlights why IoT forensics is a unique adventure and brought out the legal challenges encountered in the investigation process. A quadrant model is presented to study the conflicting aspects in IoT forensics. The model analyses the effectiveness of forensic investigation process versus the admissibility of the evidence integrity; taking into account the user privacy and the providers' compliance with the laws and regulations. Our analysis concludes that a semi-automated forensic process using machine learning, could eliminate the human factor from the profiling and surveillance processes, and hence resolves the issues of data protection (privacy and confidentiality).

Keywords**—**cloud forensics, data protection laws, GDPR, IoT forensics, machine learning.

I. Introduction

The emergence of Internet of Things (IoT) era and the ever-advancing technology in nearly all the digital gadgets indicates that the digital forensics domain is reaching a tipping point. The traditional forensic tools that worked are increasingly becoming obsolete [1]. More complex reverse engineering techniques are required as forensically relevant data is being stored in proprietary file formats. Users and criminals alike are splitting and storing data in the cloud bringing with it legal challenges (privacy and confidentiality rights) which limit the amount of data investigators can gain access to [2].

The forensics process in an IoT environment is complex. The IoT devices themselves are a challenge in the forensic realm as there are many different devices in the market [3], what makes it even more cumbersome is the lack of standardization for IoT devices. The data stored on the devices could be so little and of no historical or evidential value. The IoT devices are always connected which makes them more volatile [2]. This adds an extra layer of complexity in the forensic process. Privacy is also a key element in maintaining the confidentiality of data as it may lead to exposure of personal identified information [4].

Furthermore, [5] mentioned accountability as one of the IoT forensics challenges. The authors stress that this is because different entities manage the composition and the interactions between the IoT components. This is further argued by the authors that IoT technology is opaque due to the over usage of the IoT components thereby behaving in ways that vary from the original intention. Another key challenging aspect brought out by the authors is that the ownership, management and operation of IoT components is done by people or companies that may be of diverse geographical locations governed by their own native laws and regulations.

The integration of IoT devices brings with it the challenges related to security more so as highlighted by [6]. The authors note that confidentiality and integrity compromise is a key security and forensics hindrance. The need to assure the user that only authorised parties get access to the data is an issue. There is compromise of data integrity if unauthorised access is gained to the data.

To differentiate between Digital Forensics and IoT Forensics, a clear definition and understanding of an IoT environment is required. According to the National Institute of Standards and Technology (NIST) by [7] on IoT Cybersecurity Colloquium, it is noted that there is no common agreement on the definition of IoT. One definition from this NIST publication described IoT as things like sensors and devices (excluding computers, smartphones and tablets) that are connected through the internet to communicate and/or transmit data with or between themselves. Another definition refers to IoT as devices or things that are not fully operational computers, instead they are built for a specific purpose containing sensors which enable them to communicate through the internet. Another definition proposed by [8] IoT is defined as connecting smart devices like sensors to a network through the internet.

There are several attempts acquainting IoT, however they are generic or broad, which may not reflect the actual meaning of IoT. In this paper we consider things as devices (for example; agents, sensors, and actuators) that can communicate, detect and/or measure data with very limited or no processing power. Therefore, we define IoT as pervasive connected devices through the internet that collect, detect and/or measure data. We refer to things with very limited human control, although it could be manageable and/or configurable. Things could be

F. A. Author is with the National Institute of Standards and Technology, Boulder, CO 80305 USA (corresponding author, phone: 303-555-5555; fax: 303-555-5555; e-mail: author@ boulder.nist.gov).

S. B. Author, Jr., was with Rice University, Houston, TX 77005 USA. He is now with the Department of Physics, Colorado State University, Fort Collins, CO 80523 USA (e-mail: author@lamar. colostate.edu).

T. C. Author is with the Electrical Engineering Department, University of Colorado, Boulder, CO 80309 USA, on leave from the National Research Institute for Metals, Tsukuba, Japan (e-mail: author@nrim.go.jp).

classified based on their functionality, there are some things that can process data, while other things can detect and/or measure data and perhaps several others just observing (monitoring) data motion.

IoT forensics can be defined as a branch of digital forensics that combines three levels namely; device level forensics, network level forensics and cloud level forensics. This is explained further by [9] who stated that IoT forensics involves the investigation of IoT infrastructure (device, network and cloud). This whereby local memories of IoT devices could be investigated for potential evidence, network log files could be retrieved to reveal user activities and the cloud being a major storage of IoT device data could be a source of potential evidence.

The key players in the IoT forensic investigations are the Law enforcement agencies, IoT manufacturers, IoT users (these might be the suspects in a case) and the digital investigator (this could fall under law enforcement agency). These parties involved in the IoT forensics have different accountability and responsibilities. There are conflicting interests that emanate during the forensic process to apportion liabilities and obligations. The users have a right to privacy and confidentiality of their data that must be upheld. The law enforcement agencies in their pursuit for keeping the internet world safe, may use means like profiling and surveillance that may infringe on user privacy rights.

Most researches on how IoT relates to digital forensics is argued by [3] as being more theoretical than practical. There is a need to study and link the conflicting aspects of IoT forensics to identify potential practical solutions that overcome the challenges.

The aim of this paper is to review the current legal and technical challenges of IoT forensics by devising a quadrant model that links conflicting aspects in IoT forensics and recommending potential ways to bridge the challenges related to data protection laws and privacy.

The main contributions of this paper are: i) the emphasis of the uniqueness of IoT forensics, ii) the use of a quadrant model to expose conflicting aspects in IoT forensics process, and finally, iii) propose the application of machine learning techniques to semi-automate the IoT forensic process for profiling and surveillance.

The rest of this paper is organised as follows: Section 2 focusses on what makes IoT forensics unique. Key features related to IoT forensics are discussed and a summary of differences between traditional digital forensics and IoT forensics is presented. Section 3 looks at the legal implications in IoT forensics; the issue related to accountability is discussed. This involves regulation of personal data and legal obligations and liabilities. Section 4 expounds on the personal data in IoT by defining what personal data is, the parties responsible for personal data and the rights that users have regarding personal data. Section 5 highlights the technological approach of the research and explains that technology can be used as a tool to control and audit the forensic process. In Section 6, the quadrant model is introduced and applied to bridge the conflicting aspects of IoT forensics and to recommend and justify the use of Machine Learning to give assurance to the users on privacy concerns. Section 7 looks at the future work and finally the paper is concluded in Section 8.

II. What is unique about IoT forensics?

Forensics of IoT is still in its infancy as noted by [10]. The authors highlight that even though researchers have been attracted to this field, current Digital Forensics tools and techniques are not well equipped to handle the heterogeneous and distributed nature of the IoT setup. This has posed a challenge to the digital investigators and law enforcement agencies in the investigation process that can gather, examine and analyze potential evidence from IoT platforms and present evidence that is admissible in a court of law.

Generally, conventional digital forensics scenarios include tangible devices such as personal computers (PC), mobile phones and tablets that contain data of potential evidence. In an IoT setup, there is a significant change in the sources of evidence as there is increased number and types of devices of interest that are intangible due to different location sites, and the distributed nature of IoT, where the potential evidence may be stored on the cloud.

It is argued by [11] that the cloud, due to its convenience, scalability and on demand accessibility plays a fundamental role in an IoT forensics. The author states that with the inclusion of the cloud, the issues related to redistribution in different locations and multi-tenancy make IoT forensics different.

It is observed by [12] that in traditional digital forensics, the investigators use accepted methodologies that follow the standards, guidelines and principles provided by widely recognized bodies like; Association of Chief Police Officers (ACPO) and Scientific Working Group on Digital Evidence (SWGDE). The authors note that in an IoT setup, these methodologies may be limited due to the increased scope of IoT crimes. Recently, [13] emphasized on the privacy rights enshrined in the EU General Data Protection Regulation (GDPR) which make IoT forensics further interesting. This is because, IoT devices and their (IoT) services have a tendency of collecting, sharing and storing huge volumes of data that contains personal data that is of varied types. However, it can be noted that the personal data generated from IoT devices is unstructured and could be spoofed which makes the forensic process very challenging.

In a forensic investigation, search and seizure is a very important step. It is argued by [14] that whereas search and seizure can be easily achieved in a traditional digital forensics investigation, it becomes a challenge in IoT forensics and IoT devices are configured to work passively and autonomously. Additionally, [15] note that even though the identification of an IoT device can be done, there may be no well recognized methods or tools that can help a forensically sound process of collecting residual evidences from the IoT device.

Moreover, [16] observe that even though there could be a few methods that could be used to create forensic images of IoT devices, these methods do not adhere to the ethical considerations when evidence is being collected from the devices that are run in an environment which has multi-tenancy. These authors continue and state that while collected data could be preserved using the current techniques like hashing, the challenge in IoT setup comes in the preservation of the digital forensic crime scene. Different IoT nodes could still have real time and autonomous communication thereby making it hard to fully locate the crime scene that has been compromised.

Traditional digital forensics techniques could be used to acquire and analyse some IoT devices, there still exists a challenge of these devices possessing vendor specific software, different file systems structures and diversity of communication protocols that add complexity [3].

Another challenge mentioned by [17], is that many IoT devices do not store metadata that includes temporal information such as timestamps.

A summary of the characteristics that make IoT forensics different from other traditional digital forensics are as follows:

- More challenging due to the immense growth of IoT devices and their distributed nature,
- The IoT devices are heterogeneous in nature and require specialized tools to retrieve data,
- Existing IoT devices could be resource constrained,
- The data collected is huge and diversified, this brings complication in the forensic process,
- The proprietary protocols, laws and regulations for implementation are widely spread and not standardised.

III. Legal Implications in IoT Forensics

It is noted by [18] that the lack of universal rules and regulations coupled with standards and protocols will hinder IoT from being integrated in various organizational networks. Due to the continued use of IoT devices, there has been a rise in the creation of new regulations.

The collected data from IoT devices can be misused in a discriminatory way that goes against the user privacy, it is therefore upon the organizations who hold this data to ensure that only authorized access is granted. The inability of organizations to put in place management control measures for Internet of Things (IoT) complexities persists to be a risk concern. Policy makers have been left to scamper in finding measures to combat these security and privacy concerns.

The nature of the law is complex with many layers and is distributed across different domains meaning that there are different interpretations and application to people impacted. It therefore follows that it is difficult to assign accountability due to the complexity of IoT and the different interpretation of the law.

The independence of location of the cloud is a challenge. This is noted by [19] who state that the use of IoT devices, some of which are highly portable coupled with complex supply chains may exhibit challenges especially in determining which country's laws to use to apportion rights and liabilities.

The challenging accountability aspects in IoT environment as identified by [5] are; governance and responsibility, privacy and surveillance, and safety and security

In IoT regulations, we have brought out two areas of significance, these are legal obligations and liabilities, and regulation of personal data.

A. Obligation and Liability

For a forensic process to run smoothly, full disclosure and transparency is of utmost importance. Accountability can therefore only be apportioned if the manufacturers of IoT systems are transparent about the workings of the system. It is stated by [2] that it is within the law for a technology manufacturer whose service leads to a loss or injury to demonstrate that the actions taken were reasonable or fair, failure to which, the manufacturer faces liability.

It would be reasonable to eliminate the human element by implementing a machine learning algorithm to be run on the data and produce a report which is only to be accessed by authorised parties. However, as this approach may be acceptable by the law enforcement agencies, it may not be acceptable to both the suspects (data owner) and the Cloud Service Providers (CSP). There must be assurance of confidentiality and integrity to the data owners that their data is safe and the CSPs do also need assurance that their cloud service infrastructure is not compromised.

Transparency obligations are enshrined in the data-protection law to data subjects and regulators. When forensically assessing liability, user's liability is mostly based on negligence where no reasonable actions were taken to avert likely risks. Users are expected to be aware of the workings of a particular IoT device before using. Manufacturers are not obliged by law to explain how the developed technology works other than to keep up with the data protections requirements [2].

B. Privacy and Data Protection

The data protection laws, as emphasised by [5], are underpinned by basic principles which are; being fair, legitimate processing, being limited to the purpose , being accurate, data minimization, storage limitation , integrity, and confidentiality.

The European Union (EU) General Data Protection Regulation (GDPR) articles have a key principle of EU data protection law which stipulates that the processing of personal data should be done in a manner that is lawful, fair and transparent. As required and emphasized in the Association of Chief Police Officers (ACPO) guidelines, the forensic process must be conducted in a manner that should create audit trails that can be accessed by a third party and achieve the same results.

It is challenging to apply data protection rules on user data because technologies that generate and produce individual data have evolved dramatically with the ever growing IoT environment. It can be observed that almost all data is seen as personal data with strict rules governing personal data more so of special interest categories.

It is also difficult to apportion liability due to the dynamic supply chain of IoT which is multi-layered with multiparty ownership that could be spread across many geographical locations with different regulations of operations.

IV. Personal Data in IoT

The emergence of IoT has resulted in major concerns related to privacy, security, trust and governance. These concerns are unsurprising as they have been deemed as the potential greatest hinderance to adoption of IoT. The capability of IoT devices like CCTV to capture data that is not necessarily of the owner of the device but any other person in the vicinity without their knowledge is a breach of privacy [19].

It is noted by [20] that many issues related to the privacy and data protection have arisen from cloud services which includes government agencies accessing people's private data illegally. The other issue arising from privacy and data protection is the use of personal data for inappropriate purposes like profiling/discrimination [21]

It should be noted that huge volumes of data are collected by IoT devices, in most cases this collection is done without the knowledge of the IoT device users. The level of knowledge of these users of how their data is collected and used is very limited to enable them give free and informed consent.

A. What personal data is regulated?

Personal data is any data that relates to an identifiable living individual. This data is protected under the data protection laws. The identification of a natural person can be done both directly or indirectly through identifiers like their names, number of identification (ID number), data related to their geographical location, and or their online identity through their IP addresses. Although still personal, data can be pseudonymised (remove identifiers or replace) to help in the reduction of privacy risks which makes it hard to identify individuals. It should, however, be noted that GDPR does not cover information relating to institutions, foundations and corporations which are legal entities because their data is not personal data. Privacy rights can be referred to as the right to one's personality.

The EU GDPR data protection laws stipulate that the storing or accessing of personal data of a user held by an organization must only be consented to by the user. This therefore means that the user has to give consent for any action on their data. Article 8 of the EU GDPR in particular covers many rights related to the protection of personal data [22].

B. Who is responsible for personal data?

Controllers control the purpose and how the data is processed under the EU data protection laws. The controllers are therefore primarily responsible and liable to comply with the laws. In instances where data is processed by third parties on behalf of controllers, the third parties must abide by the regulations. In most scenarios, it is observed that the service providers are the controllers and processors of personal data.

The EU GDPR regulations have introduced huge fines for breach of user data privacy. There is direct obligation and liabilities to controllers and processors of personal data with those who breach security obligations being fined amounts not exceeding 20 million Euros or 4% of total annual turnover, whichever is higher [23].

Apportioning this liability during the IoT forensics process may be difficult to implement. This is due to many players involved and the complex supply chain which makes identification of players very hard.

C. What rights do IoT users have?

The rights of IoT users correspond to the obligations that controller must abide by when they process users' personal data. In the event of damages caused due to unlawful processing of their data, the users have a right to seek compensation. They have rights to access their personal data, refusal for their data to be processed in relation to decision making that are automated. Users can consent for their data to be processed or if the controller has a legal justification to process the data for legitimate purposes. However, under the EU GDPR regulations, conditions for valid consent may be strict because the consent has to be given freely by the user [19].

The EU GDPR regulations Article 21 gives the user the right to object. This means that, without user consent to process the personal data. data controllers must provide and demonstrate compelling legitimate reasons that override those of the users. This regulation is vague because even the very definition of compelling reasons is not provided leaving a vacuum as to how to distinguish between a legitimate compelling reason and an illegitimate one.

Article 22 of the EU GDPR data protection laws gives a user the right to choose whether or not to go through individual decision-making processes that are automated (e.g, profiling). This is also another unclear area because data controllers find it difficult in handling objections because they are forced to cease provision of all services. This leads to a situation where the users who are more concerned about privacy of their data are left with the option of either taking up the service or leaving it altogether [13].

Under the GDPR laws, data controller and processors have an obligation to inform the users of how the collection, usage, disclosure and storage of their personal information is carried out and how the users may exercise their rights over that data. A report from the UK's privacy regulator - Information Commissioner's Office [24] indicates that out of ten controllers of IoT, six don't adequately inform their customers on the usage of their personal data.

The report showed that:

i) Of the analysed devices, 59 per cent of them failed to sufficiently inform the user of how the collection, usage and disclosure of their personal data was being done;
ii) On the issues of storage, 68 per cent of the devices did not show how the data was being stored;
iii) On the user's right to be forgotten online, 72 per cent of the devices could not explain how a user could erase all their data from the devices
iv) And finally, 38 per cent of the devices did not have contact information that a customer could contact in case they had concerns related to privacy of their data.

There were concerns raised relating to medical devices used by General Practitioners (GPs). Although these devices sent encrypted emails back to GPs, there were issues infringement of data protection laws as follows:

- Through the IoT device, control is lost in the processing of data;
- The quality of users' consent is undermined as is it difficult to get it;
- The users risk losing the whole package of services from IoT service providers if they don't give consent for processing of their data in a particular way
- The original purpose for the processing of the data is possible abused as it may be processed more than required;
- The transmission of the personal data is at a high risk as the medium used may be prone to hackers who may steal the data;
- The data collected may be used in ways that were not initially intended because it collected from varied devices from different sources.

V. TECHNOLOGICAL APPROACH

It is noted by [5] that although technology is not a cure all solution in solving accountability issues in IoT forensics, it can be used to complement all the other aspects to enable come up with proper rules, regulations and standards. To better align this thought, the authors have suggested that technical means will help in:

A. Control

This entails what the determination of what happens through a process that has active steps detailing how obligations and exercise of rights are met.

B. Auditing

Auditing will make visible what happens or what happened. This will be illustrated by proving evidence explaining the operations of the system, actions and the recourse thereof. It is at auditing that digital forensics plays a major role in revealing what transpired in an event of loss of data, data breach or damages.

Control and audit augment the accountability considerations. The auditing will increase transparency in the IoT systems giving rise to informed decision making by users and provide evidence that can be very useful in investigation processes to apportion liability [5].

VI. QUADRANT MODEL

To aid this paper further, a quadrant model developed by [25] was used to help understand different scenarios at play in IoT forensics and propose a solution to the privacy, confidentiality and data integrity for a sound IoT forensic investigation process.

A quadrant model tries to complement conflicting elements in a social phenomenon. It relates to how different aspects ranging from law to social norms affect those involved. In most cases, these aspects are acceptable and effective, some aspects might be unacceptable but effective, others may be acceptable but ineffective and lastly aspects may be unacceptable and ineffective.

This paper uses this quadrant model and equates the acceptable and unacceptable elements to admissible and inadmissible (in a court of law) respectively as illustrated below in Fig. 1 *Quadrant Model*.

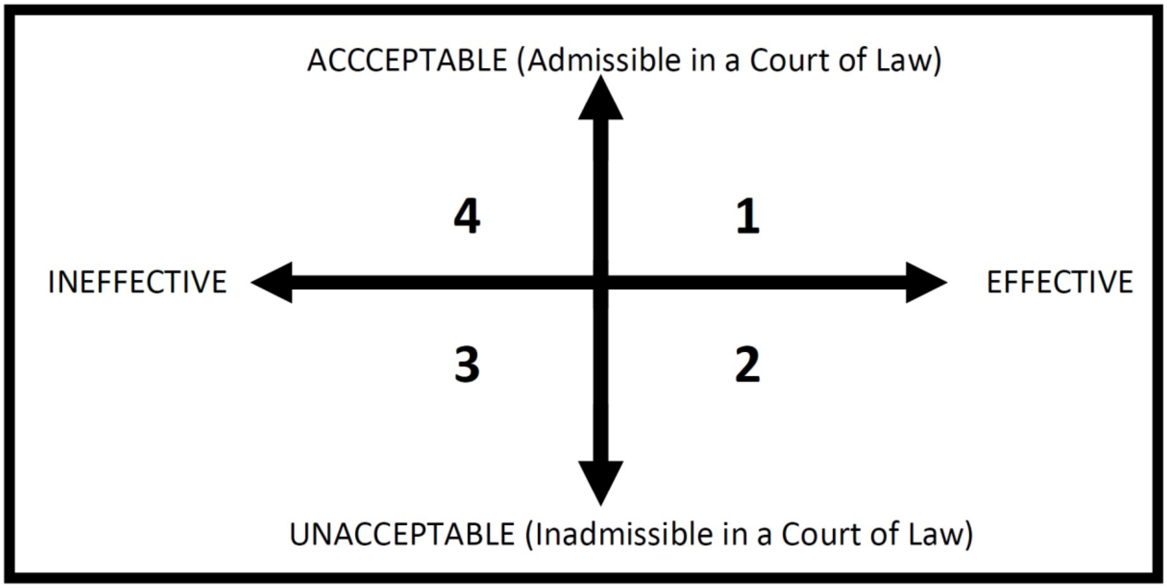
ACCCEPTABLE (Admissible in a Court of Law)
4
1
INEFFECTIVE
EFFECTIVE
3
2
UNACCEPTABLE (Inadmissible in a Court of Law)

Fig. 1 Quadrant Model

Quadrant 1 indicates actions that are effective and legally acceptable to all parties involved. These elements are compliant with the laws and therefore lead to an admissible report in a court of law. These can be for example, auditing and control, safety and security, confidentiality and privacy, data protection, and transparency.

Quadrant 2 is the problem area, consists of actions that are effective in increasing efficiency, but where parties have conflicting views. The activities involved in this quadrant are for example the use profiling, surveillance, tapping, eavesdropping and cloning among many other inadmissible mechanisms. Law enforcement agencies may want to employ those mechanisms as a security measure; however, users may claim that their privacy is encroached, data being accessed by unauthorized entities. This may lead to issues related to legal obligations and liability between IoT users and IoT manufacturers.

Quadrant 3 consists of actions that are generally inadmissible in a court of law and at the same time ineffective. For these reasons, this quadrant will be ignored as it is unproductive

Quadrant 4 are actions which are admissible in a court of law but do not contribute to increased efficiency. These elements are not admissible in a court of law. These actions can be for example, regulators banning some IoT devices and enforcing licensing for IoT devices. These actions, although admissible, they may be hard to implement meaning that they will be so ineffective and unproductive. This paper ignores the actions in this quadrant.

A. The Quadrant Model in Context

As the quadrant model is to complement conflicting aspects or interests, it is evident from this paper that the conflicting parties in an IoT forensic investigation process are the users of IoT, manufacturers of IoT platforms, IoT service providers and Law enforcement agencies. All these parties have conflicting interests in that, whereas the law enforcement agencies may want to do profiling and surveillance on user activities, they are restricted by law as it is an infringement to the privacy and confidentiality of the user.

IoT Service Providers and IoT manufactures alike may also install backdoor applications onto IoT devices to snoop on user activities and in most cases collect users' private data for marketing purposes. The IoT Services Providers and manufacturers deny this wrongdoing whenever an investigation comes up. They blame users of negligence and would not also allow forensic investigators get to underlying structure of the technology used their devices even though they are expected to be transparent in their undertakings.

These conflicting aspects or interests put in context complicate the IoT forensic investigation process.

In the digital forensics' domain, forensic investigators are required to carry out their investigative process in a manner that is legally acceptable/admissible. The law enforcement agencies are also required to work within a specified terrain of regulations. All these activities are to be done without infringing the rights of a suspect.

This paper therefore uses the quadrant model to find reasons as to why and how the inadmissible but effective actions can be made effective and admissible in a court of law. Particularly, this is to show cause why profiling can be acceptable by the user and be effective to the law enforcement agencies and be admissible in a court of law, as illustrated in Fig. 2 *Profiling and Surveillance in IoT Forensics***Error! Reference source not found.** below.

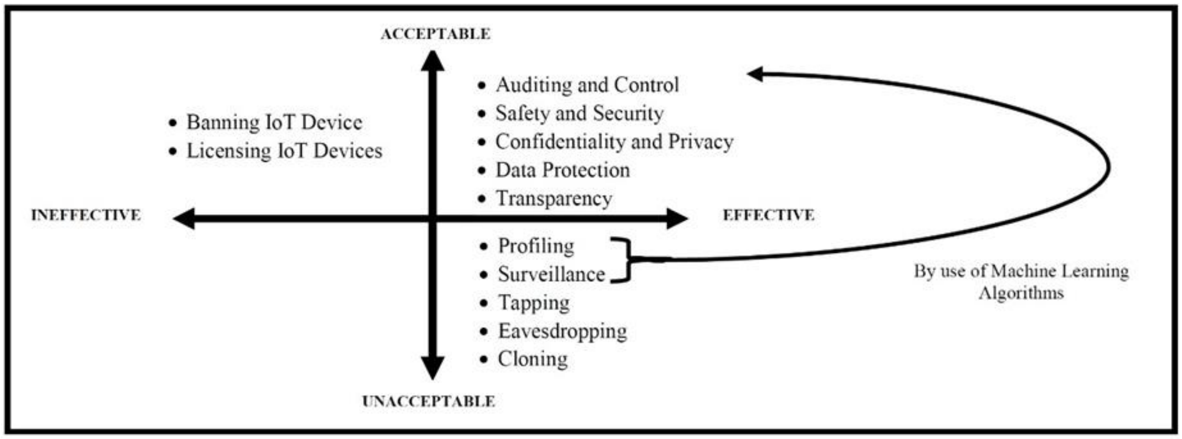

Fig. 2 Profiling and Surveillance in IoT Forensics

B. *Profiling and Surveillance in IoT Forensics*

Profiling and surveillance are useful means (when used lawfully) through which law enforcement agencies can use to detect any security threats that are posed by IoT gadgets. As earlier highlighted in this paper, IoT data is transmitted to the cloud. The cloud therefore serves as a platform through which a profiling or a surveillance mechanism can be deployed for profiling and surveillance to give alerts or reports. This paper proposes the use of Machine Learning algorithm as to implement this mechanism.

C. *Why Machine Learning for Profiling and Surveillance?*

As explained by [26] and [27], with experience, Machine Learning programs have the capability to improve automatically and learn without being explicitly programmed.

The use of Machine Learning for profiling and surveillance is to eliminate the human factor and give the owner of the data the confidence for their privacy and confidentiality, thereby only ensuring only authorized access of the data is gained.

The human decision making as observed by [28] is in most cases influenced by behaviours like stereotyping and prejudice. Some people make decisions based on the characteristics of profiles they perceive. This may distort evidence as it may be inaccurate, incomplete or none thereof because it may be wholly derived from stereotype and prejudice [29].

Machine Learning being a science that consists of algorithms that can detect patterns in data and as highlighted by [30], different profiles of individuals can be created through probabilistic processing of their personal by use of Machine Learning. This paper argues that Machine Learning algorithms can be deemed appropriate to be used in profiling and surveillance.

It is also noted by [2] that profiles only represent a version of reality which in some cases may not be the exact reality which is created from a process of data mining that includes algorithms and data used in the process.

VII. Future Work

The future work from this paper is to design a Machine Learning algorithm that can be implemented in the cloud for profiling and surveillance and as a forensics tool to semi-automate the process of investigation and eliminate a situation where decisions making processes are only based on human beings.

To investigate ways in which all the standards, rules and regulations related to IoT forensics can be formalised and standardised to aid in the investigative process.

It is also desirable to carry out an in-depth analysis of the EU GDPR rules and how these laws relate to the use of Machine Learning algorithms in the process of decision making that is automated and the effects it has on users and the final judgement.

VIII. Conclusion

Plethora of digital things is encircling our world and shaping our life, they took their place in the harmonious complexity of the world. These things are connected pervasively through the internet in a very complex structure which may cause many challenges.

This paper highlights the need for more advanced mechanisms for handling IoT and cloud forensics. This area is multi-layered and complicated as it has many players and needs more cooperation between parties involved.

The laws and regulations in place further make it a bit hard for law enforcement and forensic investigators to carry out their work as the issues of privacy and confidentiality come in to play. The lack of comprehensive, widely accepted international standards, rules and regulations to manage the IoT and cloud security are a big concern. as we continue to witness more complexity in IoT technologies with no laws to govern.

A concerted effort between multi-disciplined experts should be mooted to consolidate the main areas of conflicts and provide viable solutions for long term security measures. These efforts should consider the development of unconventional digital forensic technologies to improve the effectiveness of the whole investigation process as well as to increase the degree of the acceptance of the parties involved in the IoT forensic process.

Law enforcement agencies should carry out public awareness forums (using any reasonable medium) and educate the general public on the responsibilities they have to ensure they are safe online. Many IoT users fall prey to security scams because they are ignorant or negligent.

Whereas Machine Learning algorithms can be deemed resourceful in generating timely and accurate reports, it should be noted EU GDPR regulations state that the final decision on a person's character should not be made solely relying on the automated process that violates the person's interests.

Overall, it should be noted that using semi-automated decision-making process especially that of Machine Learning algorithms in profiling and surveillance is a sure bet of eliminating human elements that bring with them discrimination, stereotypes and prejudices.

References

[1] S. L. Garfinkel, 'Digital forensics research: The next 10 years', *Digit. Investig.*, vol. 7, no. SUPPL., 2010.

[2] S. N. Silva, C. Reed, and E. Kennedy, 'Responsibility , Autonomy and Accountability : legal liability for machine learning', no. 243, pp. 1–31, Oct. 2016.

[3] V. S. Harichandran, F. Breitinger, I. Baggili, and A. Marrington, 'A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later', *Comput. Secur.*, vol. 57, pp. 1–13, 2016.

[4] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, 'Privacy in the internet of things: Threats and challenges', *Secur. Commun. Networks*, vol. 7, no. 12, pp. 2728–2742, Dec. 2014.

[5] J. Singh, C. Millard, C. Reed, J. Cobbe, and J. Crowcroft, 'Accountability in the IoT: Systems, Law, and Ways Forward', *Computer (Long. Beach. Calif).*, vol. 51, no. 7, pp. 54–65, Jul. 2018.

[6] R. Mukundan, S. Madria, and M. Linderman, 'Efficient integrity verification of replicated data in cloud using homomorphic encryption', *Distrib. Parallel Databases*, vol. 32, no. 4, pp. 507–534, Dec. 2014.

[7] K. Megas, B. Piccarreta, D. Gabel, and O. 'rourke, 'Internet of Things (IoT) Cybersecurity Colloquium A NIST Workshop Proceedings', Dec-2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8201.pdf. [Accessed: 01-Oct-2018].

[8] Z. A. Baig *et al.*, 'Future challenges for smart cities: Cyber-security and digital forensics', *Digital Investigation*, vol. 22. pp. 3–13, Sep-2017.

[9] S. Zawoad and R. Hasan, 'FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things', in *Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015*, 2015, pp. 279–284.

[10] V. R. Kebande and I. Ray, 'A generic digital forensic investigation framework for Internet of Things (IoT)', in *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, 2016, pp. 356–362.

[11] A. Induruwa, 'Hidden in the clouds: The impact on data security and forensic investigation', 2011, pp. 77–77.

[12] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, 'Internet of Things Forensics: Challenges and Approaches', in *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, 2013.

[13] S. Wachter, 'Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR', *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 436–449, Jun. 2018.

[14] M. Harbawi and A. Varol, 'An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework', in *2017 5th International Symposium on Digital Forensic and Security, ISDFS 2017*, 2017, pp. 1–6.

[15] C. J. D'Orazio, K. K. R. Choo, and L. T. Yang, 'Data Exfiltration from Internet of Things Devices: IOS Devices as Case Studies', *IEEE Internet Things J.*, vol. 4, no. 2, pp. 524–535, Apr. 2017.

[16] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, 'Internet of Things security and forensics: Challenges and opportunities', *Future Generation Computer Systems*, vol. 78, pp. 544–546, Jan-2018.

[17] A. Dehghantanha and K. Franke, 'Privacy-respecting digital investigation', in *2014 12th Annual Conference on Privacy, Security and Trust, PST 2014*, 2014, pp. 129–138.

[18] C. P. Chike, 'The Legal Challenges of Internet of Things Mass Communications View project Cybersecurity Law View project', 2018.

[19] W. K. Hon, C. Millard, and J. Singh, 'Twenty Legal Considerations for Clouds of Things', Jan. 2016.

[20] I. Walden, 'Law Enforcement Access to Data in Clouds*', in *Cloud Computing Law*, Oxford University Press, 2014, pp. 285–310.

[21] A. Collins, A. J. Fleisher, R. Freeman, and A. Maughan, 'SCL: The Internet of Things: The Old Problem Squared', 2014. [Online]. Available: https://www.scl.org/articles/3055-the-internet-of-things-the-old-problem-squared. [Accessed: 24-Oct-2019].

[22] J. Kokott and C. Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', *Int. Data Priv. Law*, vol. 3, no. 4, pp. 222–228, Nov. 2013.

[23] European Union, 'Regulation, G. D. P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing D', *Off. J. Eur. Union*, vol. 59, no. 294, pp. 1–88, 2016.

[24] P. Commissioner, 'International study finds privacy shortfalls in Internet of Things devices', 2016.

[25] B. Godfrey, 'Electronic work monitoring: An ethical model', *Sel. Pap. from Second Aust. Inst. Comput. Ethics Conf.*, vol. 1, no. figure 1, pp. 18–21, 2000.

[26] T. M. Mitchell, 'Machine Learning', *Computer (Long. Beach. Calif).*, vol. 2005, no. April, p. 414, 1997.

[27] J. Copeland, 'AlanTuring.net What is AI?', 2000. [Online]. Available: http://www.alanturing.net/turing_archive/pages/reference articles/what is ai.html. [Accessed: 24-Oct-2019].

[28] D. Kamarinou, C. Millard, and J. Singh, 'Machine Learning with Personal Data', Nov. 2017.

[29] M. Hildebrandt, 'Defining profiling: A new type of knowledge?', in *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Netherlands, 2008, pp. 17–45.

[30] M. Hildebrandt, ‘Some Caveats on Profiling The Onlife Initiative View project Smart Technologies and the End(s) of Law View project’, *Data Prot. a Profiled World*, pp. 31–41, 2010.