International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 9, Issue 3, May - June 2020 **ISSN 2278-6856**

Brief Overview of Existing Challenges in IoT Forensics

Mr. Raihan Patel[1], Dr. Zakiyabanu Malek[2]

[1]Institute of Forensic Sciences, Gujarat Forensic Sciences University

[2]Faculty of Computer Technology, GLS University

Abstract: ***The Internet of Thing enables a platform which allows communication and connection of billions of devices at the same time. The technology provides various benefits for consumers that alters how their user leverage the technology. Many Possible legal as well as many technical challenges comes with such expansion within IoT ecosystem in the field of IoT Forensics. There are many underlying issues that must need to be overcome in order to have an effective IoT investigation. The purpose this paper is to present an overview of the IoT concepts, digital forensics and point out the existing challenges with IoT forensics. Furthermore, Various possible solutions that are proposed in recent research are examined as well.***

Keywords: Internet of Things(IoT), Digital Forensics, IoT Forensics, IoT Forensics Challenges

1. INTRODUCTION

With every revolutionary invention, The internet is constantly transforming into newer and newer types of applications, to the point that, Now, Nobody can avoid it. The kind of communication that takes place now is either human-device communication or human-human communication through devices. However, With the introduction of Internet of Things, We now have a promising future that could deliver a machine to machine (M2M) communication. The concept of Internet of Things was first included by Ashton in 1999, according to whom, "The same potential to change with the world can be seen in The Internet of Things, just as the Internet did. Maybe even more so".Afterwards, The international telecommunication Union presented the first formal presentation of the IoT in 2005. As per International Telecommunication Union, IoT can provide a global infrastructure for the information space, where it can enable advance services based on the existing and evolving information and communication technologies.

The IoT enables billions of things to communicate and connect at the same time. The technology provides various benefits for consumers that alters how their user leverage the technology. A collection of interconnected devices and low-cost sensors make it possible for information to be collected from our environment, thus in turn makes day-to-day life easier.

The IoT is very much in trend at the moment in the cyber space. That resulting in it drawing minds from both academic institutions and businesses. The technology is undoubtedly powerful enough to alter our living. In comparison to the adoption of landline phones and electricity, the rate of IoT adoption is at least five times higher. Cisco predicted in 2016 that, in Next 15 years, 500 billion devices will be linked up to the Internet. Given the current technology, All of these devices comes with sensors that are responsible to collect data, engage with the environment and communicate using internet. With the way technology is being used today, These activities are becoming the important member of the future of the internet, which enclose diverse range of services and application. These IoT devices are connected to each other using various communication methods such as mobile devices, networks which are either wired or wireless.

Recent years have seen an accelerated use of IoT Technology. These smart devices have being used in major fields like health-care, smart city projects, smart-phone manufacturing, wearable smart devices, transportation, etc. A lot of concerns regarding the various vulnerabilities of the technology also came with its growth. Because IoT at it's core was never developed with security in it's core. Which is resulting in cyber-crimes being committed using these devices. The number of cyber crime incidents linked to IoT devices are causing serious concerns. According to a recent report shared by RBI, India, There were in total 2059 cases recorded of cyber fraud in 2017-18 which amounted around 109.6 crores INR. The numbers were around 1,372 in 2016-17 amounting to 42.3 crore INR. Apart from that, India has seen 22% rise of attacks in IoT ecosystem across the country compared to last quarter. Symantic also stated recently in their security threat report that there is a huge chance of rise in cyber crime cases related to IoT ecosystem. Incidents including Malware attacks, Phishing and Pharming Attack, SQL injection, and various attacks have been detected. Such attacks can be done either by employing the IoT device itself or by exploiting the known and unknown vulnerabilities of the device. Here, The main difficulty is that, All these devices are connected to each other through the network, meaning it is extremely difficult to conduct static digital forensics using the traditional methodologies, at least it is much more complicated that conducting other traditional computer forensics. Real-time investigation of the device is necessary in order to carry out proper IoT forensics because of the limitations of the IoT devices and the volatile nature of the digital evidences that can be found in IoT ecosystem.

The aim of this paper is to review the current scenario in Internet of Things regarding it's digital forensics areas, and to discuss the existing challenges linked with it while building the direction for future research. Section 2 discusses the present view of Digital Forensics while Section 3 discusses brief about IoT Forensics. In Section 4, The discussion focuses on the currently available frameworks for IoT forensics. Following that, The discussion move towards the current challenges faced by researchers in IoT forensics. Finally, a conclusion and future research is presented in Section 6.

2. Process of Digital Forensics

Around 1960s, When technological revolution was taking place, We have seen significant growth in the number of crimes committed either using computers or on computers. Due to the crime rates in cyber space, Digital forensic was a much needed field to fight the combat against cyber crimes and also to upgrade legal evidence discovery on digital platforms. As per the definition offered by NIST, digital forensics is the use of science to identify, collect, examine, analyze and presenting digital evidences, But examiner must maintain the integrity of the data and the chain of custody of each evidences collected from the crime scene and afterwards.

Over the years, It has been widely accepted that there is not one single forensic procedure on its own which can be adhered to in every digital investigation. Basically, No framework for digital forensic process exist that can be used as complete solution for the existing challenges. However, There are numerous popular standards available which applicable to the general digital forensics process, such as: IDIP, DFRW, NIJ and NIST. Numerous experts of the field across the globe have reached on an accepted process of NIJ, which are set out something like this :

- Assessment : In order to decide which course of action should be taken, The forensic examiner who is specialized in Computer Forensics should analyze digital evidences unerringly.
- Acquisition: In it's true form, Digital Evidences are very delicate and can easily be altered, damaged or destroyed if they are not taken care of properly. The best practice that is carried out across the world is to not examine the original evidence but to examine the copy of the original evidence. Apart from that, original evidence should be obtained in a way that make sure the protection and preservation of the integrity of the evidence.
- Examination: The process being discussed here seeks to draw out and assess digital evidence. Extraction is simply the recovery of data from its media.
- Analysis: Interpretation and Presentation of said data in a format which is useful and makes sense is what analysis is all about.
- Documenting and reporting: It is no secret that documentation is one of the most if not the most important part of any forensic procedure. It is must to document anything and everything including each observation of examiner and each action taken by examiner during the whole process. A report should be detailed in writing which culminate and compile each findings.

3. Process for Internet of Things Forensics

Internet of Things is a new and trending technology in the cyber space which has came in with uncommon, exclusive and complicated challenges for the overall digital forensics process. Estimation made by many researcher state that the number of networked devices will stand at 50 billion by the end of 2020, and said devices will produce a substantial amount of data. Processing of that much IoT data will lead to a comparable rise in load for data centers. That basically means that providers are left to deal with new challenges related to their capacity, security of the data and big data analytic techniques. The biggest challenge here is to ensure data is being handled conveniently, Since any application that works on IoT platforms completely depends on the data management service's properties.

It has been stated that Internet of Things forensics consists of a mix of multiple fields of Digital Forensics : Device Level Forensics, Cloud Forensics, Network Forensics.

- Device Level Forensics: In any given scenario, an examiner may need to extract data from the IoT devices, and specially extract data from the device's local storage. The device level forensic can be applied when such need is arised. Because such evidence can play a vital role in the overall IoT Forensic Examination Process.
- Network Forensics: We have already stated it couple of times that all the devices in IoT environment are going to be interconnected. Such scenario leave examiners with a possibility to find many vital evidences from the network in which the said devices are connected. Using the logs collected from networking devices, it may be possible to find source of attack or to identify the attack itself. Such evidences can serve as a vital tool to declare a suspect either guilty or not guilty. The IoT platform is comprised of various forms of networks, e.g. Personal Area Network, Body Area Network, Wide Area networks, home Area Number and Local Area Networks. Crucial piece of evidence can be extracted from any of these networks.
- Cloud Forensics: Given the limited possibility of storage that comes with IoT devices, Cloud platform has a crucial role in the IoT space. That makes Cloud Forensics an important field to not leave unexplored for IoT forensics. Currently available majority of IoT devices have low computational and storage capacity, Manufacturers store data that is generated from IoT devices and IoT networks in the cloud. Mainly because Cloud solution provide various benefits such as considerable capacity, easy scalability and accessibility on demand.

Indeed, Many researchers have attempted for a model developed to deal with the unique characteristics of IoT, but even after that, There are still plenty of challenges which we still don't have solutions for. A good example can be, the underlying complexity which comes when examiner tries to extract data from the IoT platform, The task becomes near to impossible for investigators to deal with devices to generate evidences that are admissible in the court of law and are solid in terms of forensics. The above-mentioned complexity comes with many existing challenges such as ambiguity regarding the source of the data and the location where it is stored, The fact that traditional existing digital forensics becomes inapplicable in IoT space, ensuring Chain of Custody's integrity, and the formats of data as different company uses different forms to generate and store the data. Due to all this, The IoT forensics is very much young field and there are many stones unturned, specifically because of the said challenges that exist and the limited amount of research work that can be found.

4. Existing Forensic Frameworks

Plenty of researchers have dedicated their research towards the difficult task of making IoT Forensics effectively possible. For that, a framework was named The Digital Forensic Investigation Framework for IoT(DFIF-IoT) was proposed, The biggest advantage the framework had was that it provided strengthening of the abilities for the investigators and provided a high certainty level. The biggest advantage of the said framework is that it adheres to the ISO/IEC 27043 2015 - an internationally accepted standard for processing information technology techniques that is being used for security and the principles of incident investigation. The paper published by the author the qualitative methods gathered shows that incorporating the DFIF-IoT into tools used for digital forensics in the future can help in providing efficient forensic crime investigation in the area of IoT.[1]

Kebande and co-authors have come up with a unique framework named CFIBD-IoT; this cloud-based framework comprise three parts that is what makes it unique. It has a digital forensic investigation layer, a cloud infrastructure layer and a forensic evidence isolation layer. The standardized mechanism must be adopted for the extraction and preservation of the evidence such as ISO/IEC 27043 was the main recommendation made by the paper. [2]

A practical approach with a general framework for IoT forensics via device state acquisition was proposed by Meffert and co-authors. In the said work that they carried out. The researcher explained that it is completely possible to collect and log IoT state data on the go by employing a Forensic State Acquisition Controller, that makes it possible to obtain data directly from cloud, an IoT device or even from controllers. The researcher here integrated NEST open APIs in order to extract data regarding the state of the Nest thermostat on any occasion when data is transferred to the cloud. The researcher have also provided a proof of concept implementation. They did that by setting up openHAB and created a script which can mimic a FSAC implantation. The results obtained by these researchers showed that practically extracting state data, which as a matter of fact forensically relevant, from Internet of Things device is a reality.[3]

Hossain and co-authors came up with framework called FIF-IoT - a forensic investigation framework which employs a public digital ledger to focus on the facts in crimes which take place within IoT systems. The said framework provides a feature to extract and store evidence in various forms of interactions like D2C(Device to Cloud) or D2D(Device to Device) or D2U(Device to User). The evidence is then kept in a public ledger. The FIF-IoT framework is capable of providing the CIA of the publicly available evidences. The said framework can also be used as a platform where integrity can be checked for the evidences that are acquired throughout the investigation process. Researcher has also presented a case study of an adverse scenario. Researcher showcased that FIF-IoT is tamper-proof against a potential collusion scenario. In the said research, author tested the prototype of the framework to evaluate the performance. [4]

Chi, Aderibigde and Granville suggested the use of a framework designed for the acquisition and analysis of IoT data. The basic goal of the propose framework was to collect data from various IoT devices. The aim here was to provide an evidence format which can be centralized for better investigation and to compile events that took place in cloud-based setting. The approach put forth by the researcher is to provide the user with a mobile based application which can pull data from the android device; then the artifacts extracted are stored in a centralized evidence format, while the second part of the framework which is a desktop application aids in by creating a timeline to make analysis of all the collected evidence possible. [5]

Chhabra and co-authors proposed a possibility aiming at big data analysis and forensics, with exceptional precision and sensitivity. They proposed a generalized forensic framework which had the programming model of Google known as MapReduce at it's core. That helped the framework achieve traffic translation, extraction and the analysis of dynamic traffic features. They also included tools that were open source in nature to support parallel processing and scalability. They included comparative analysis of ML models that are being used for P2P malware analysis in mocked on-the-go. A data-set from CAIDA was implemented in parallel so that the proposed model can be verified. The findings showed that the model had sensitivity of 99% in forensic performance metrics. [6]

Al-Masri, Bai and Li proposed a Fog-based Internet of Things framework that is able to check and mitigate cyber attacks which target Internet of Things systems during the beginning phase. Author was inpired by the DFRWS investigation model for the proposed framework. [7]

IDFIF-IOT (Integrated Digital Forensics Investigation Framework) was proposed by Kebande and co-authors for the IoT ecosystem. The proposed framework is actually a newer version/ extended version of DFIF-IoT(Digital

Forensic Investigation Framework for Internet of Things). The porposed framework comes with an aim to provided a methodology complete with techniques that are widely accepted and are being used in the process of digital forensics and are also capable of PDE(Potential Digital Evidence) analysis which are generally being generated by the IoT ecosystem devices. Often, PDE can be used as a sole evidence to provide a fact and that makes the proposed framework an effective extention to DFIF-IoT. [8]

A digital forensic framework for smart home and official appliances was proposed by Leonardo and co-authors named IoTDots. There were mainly two main components in IoT Dots. First is IoT Dots modifier and Second is IoT Dots Analyzer. During the time of compilation time, The source code analysis of the smart application is done by IoTDots modifier and it tries to insert tracing logs automatically. Afterwards, during the run-time, the generated logs are stored in a database created by the proposed framework. During the process of forensic investigation, IoTDots analyzer can used by the Examiners. The proposed framework applies data processing and machine learning to find forensically valuable information from the IoT devices. Research tested the proposed framework in a smart office scenario where researcher setup total 22 devices and sensors. Researcher also considered 10 different cases of forensic activities and behavior from users, apps and devices.[9]

Mohammad Qatawneh and co-authors proposed a Digital Forensic Investigation Model for IoT(DFIM). The DFIM comes with two components: DPZ(The Data Provider), which is tasked with looking after the collection of data gathered by sensors into a set of groups, In which, each group contains data or documents related to each other, and the investigation authority which looks after receiving the requests from the claimers for investigation, check the validation of the request and finally select the appropriate investigators. With the aim to improve IoT forensic investigation process, The proposed DFIM consists of seven stages and take into consideration a set of principle regarding security, privacy, accuracy, performance, data reduction, Openness and transparency.[10]

As discusses, Numerous frameworks have been proposed to deal with the unique characteristics of the IoT forensics, Still there are still many challenges which are needed to be resolved. Below, discussion focuses on some of the important challenges faced by the field of digital forensics in IoT environment.

5. IoT Forensics Challenges

In a very near future, IoT will be present in all the aspect of our life, from taking care of homes to managing entire cities. While this does make humans lives easier, the same also gives rise to numerous issues regarding the security of the ecosystem and also the forensics. Here, The discusses focuses on brief review of the key forensic challenges encountered in IoT environment.

5.1 IoT Device Storage Limits

Often Manufacturers keep IoT devices with very limited computational and memory capacity. Which basically means that the lifespan of data in IoT devices is very limited and can be easily overwritten, which could result in loss of evidence. Forensic Process for devices with very limited or no storage involves a huge challenge. One more challenge is the amount of time for which the evidence will stay in the device before being overwritten by the new data. It is a common and easy for IoT applications to leverage cloud solutions for storage to store the data. Which could basically keep the data stored for longer time of period. Due to this, Cloud Storage can be considered as an easy solution. However, That solution would come with another problem and that is, How can investigator prove that the evidence has not been altered with or modified.

5.2 Cloud Forensics

Majority of the application which are being used in Cloud Environment and also considering the limitations of computing and storage capacity of IoT devices basically means that the cloud is where the majority of the information stuff is stored. The help of CSP (Cloud Service Provider) is needed in order for the examiner to acquire evidences from the Cloud environment. In majority cases, these CSP are very hesitant to co-operate and share the information or providing investigators with access to their cloud environment. One thing to note here is that, Handling of digital forensic evidence on cloud differs based on the cloud platform such as Software as a Service, Platform as a service or Infrastructure as a service. In SaaS and PaaS, The method used to extract evidence primarily involves service providers, while in IaaS, Client’s involvement is required along with the service provider. That comes with a challenge. It is never going to be easy make client and service provider both co-operate. Examiner also need to take into consideration that cloud computing is distributed in terms of its nature; Examiner and research need to come up with methods that are also adaptive to the changes in the way data and applications are deployed to accommodate this distributed behaviour. Due to this distributed nature, A huge amount of IoT based data is scattered across different locations and often those locations are not necessarily in the control of the users. In any given scenario, These data could be in the cloud, with a third party, on a mobile phone or on other devices. Finding where evidence is stored in such scenario has been considered as the biggest challenge that an investigator can face while trying to carry out investigation. It is completely possible that IoT data might be kept in different countries and mixed with other users information as well. Which basically means the regulations and law of different countries may get involved.

5.3 Complexity and Diversity of the ecosystem

Every mainstream and growing manufacturers are investing their resources in terms of money and research to bring newer IoT devices to market that can make our lives trendy and easier. Even Service Providers have now also came up with various offers and services for customers.

Devices being launched are coming with various operating systems and are capable of connecting to many different network technologies simultaneously. With features like dynamic and interactivity present, the IoT becomes exponentially complex and near to impossible to understand. Such situation can easily result in rise of exploitation on the part of adversary.

The next complexity comes with the way manufacturers store the data in the device as file formats that are used to store data that could be helpful forensically are becoming proprietary and are very complex when it comes to reverse engineering it. It is a common practice in such ecosystem to break the data in to smaller components and store them in various locations.

Another challenges come with the legal aspects that basically limits the amount of data forensic examiner can actually access.

IoT covers a vast field of devices which also comes as a difficulty for forensic examiners as all those devices have very different architecture going with them and it is not possible at the moment to have a framework that could do the forensics of all these devices using a single platform.

Along with that, The communication protocol that IoT devices uses are also very different from one another like MQTT, WiFi, RF or ZigBee. Such challenges makes it hard for examiner to extract artifacts out IoT ecosystem the way they extract it from general devices.

5.4 The chain of Custody

The chain of custody is considered to be the crucial aspect of any forensic process. It basically helps guaranteeing the acceptance of the extracted evidences in the court of law. The chain of custody provides the information about complete history of the evidence during all the stages of the investigation process from the collection to presentation. The chain of custody is used to prove the integrity of the digital evidence and if it can successfully prove that then only court would accept that digital evidence as a legitimate one. The chain of custody also provide information about where, when and who came into contact with the collected digital evidence throughout the process. Given the complexity of evidences and their location in IoT ecosystem, it is really challenging to prove in court of law that the integrity of the collected evidence was maintained throughout the process.

5.5 Existing Tools in the field

Given the fact that IoT is a new world, Majority of the tools and framework that exist for the forensics of IoT comes with plethora of limitations and they are simple not updated at the same pace as the IoT technology itself. The current traditional tools that can be found in the field of General Digital Forensics are proven to be not able to cope up with the infrastructure of the IoT environment. Examiner can surely use a mix of network, computer and cloud forensic tools to obtain forensically relevant data from IoT environment. It is possible to incorporate network forensic tools to gather any data that one IoT device sends to another through a networking medium. Certain commercial tools do exist like EnCase and FTK that can be used to obtain evidences successfully up-to some extent. Still, Not one tool is capable of effectively carrying out entire IoT Forensics process efficiently. Due to this, There is a huge need of a tool that examiners can rely upon and is affordable at the same time. Such tools need to be capable enough to obtain and analyse forensic evidences with integrity in mind in order to provide effective forensic process to the examiners.

5.6 IoT Forensic Process

From what has been discussed so far, The examiners do faces numerous challenges during the process of IoT forensics. IoT devices are often designed in a manner that they could function in autonomous passive manner, which makes it harder for examiner to detect their presence. Even if Examiner manages to identify and detect the presence of IoT devices, often there are no reliable documented methods or tools that exists to gather proper evidence from the device that can be presented as forensically solid evidence in the court. One challenge that examiner often face in IoT ecosystem is to preserve the crime scene,Where various nodes and sensors are constantly communicating with each other in real-time. That basically makes the task near to impossible for examiner to identify boundaries of a crime scene. Majority of the nodes that exist in the IoT ecosystem do not store any kind of meta-data, which makes it hard for examiner to prove the credibility of the evidence collected. Correlation becomes an impossible task if no meta-data exist like modification related time-stamp, Access time-stamp, creation time of the data. Since Majority of the IoT devices are designed to be used for personal usage, The kind of data they collect and store is personal as well, Which is an issue for examiner as now they need to consider privacy of the data as well while doing analysis and correlation of the collected data.

5.7 Security Aspects of IoT

Manufacturer never designed the IoT devices with security in mind, mainly because IoT was never considered to be a field where crimes would be committed, Which makes IoT devices vulnerable to numerous security issues, with each day hacker potentially being able to find new vulnerabilities. Here are some of the security related issues that can be found in IoT ecosystem: A type of attack that attempts to communicate on behalf of a legitimate thing in an unauthorized way, A type of attack where attacker modifies or deletes the data that is existing on an IoT device thus making the evidence collected from that device pretty useless for the examiner, All IoT devices comes with a possibility to remotely monitor and configure them which makes it possible for an attacker to attempt to obtain unauthorized access and take over the control of the device as well as the data it stores, An attacker can also flood the network with the amount of traffic that the network cannot handle and it would result in exhaustion of the resources which basically makes the network unavailable to the users.

6. CONCLUSION

High probability of cyber threats are coming with the increasing amount of connected devices day by day. The underlying issues have already been identified by researchers which examiners are facing while they carry out forensic process for any case that is related to Internet of Things. Given the fact that IoT is a new field, We yet to have proper tools and technology that can make the forensic process easier for the examiners. With the existing tools that are available for IoT forensics, There are many challenges and issues that still need resolutions. The paper presented here has tried to discuss the existing IoT and Digital Forensic technology and tried to put some light on the existing challenges that are needed to be solved in order to have an effective digital forensic process for the Internet of Things ecosystem. Further studies are needed to be carried out on various aspects like effectiveness of IoT forensic framework, consideration of privacy, integrity and storage of the collected data. Such IoT forensic tools can help examiner carry out effective digital forensic process on the Internet of Things devices.

REFERENCES

[1] V. R. Kebande and I. Ray, "A Generic Digital Forensic Investigation Framework for Internet of Things (IoT)," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, 2016, pp. 356-362, doi: 10.1109/FiCloud.2016.57.

[2] Kebande, V. R., Karie, N. M. and Venter, H. S. (2017) ‘Cloud-Centric Framework for isolating Big data as forensic evidence from IoT infrastructures’, in 2017 1st International Conference on Next Generation Computing Applications (NextComp), pp. 54–60.

[3] Meffert, C. et al. (2017) ‘Forensic State Acquisition from Internet of Things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition’, in The 12th International Conference on Availability, Reliability and Security.

[4] M. Hossain, Y. Karim and R. Hasan, "FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger," 2018 IEEE International Congress on Internet of Things (ICIOT), San Francisco, CA, 2018, pp. 33-40, doi: 10.1109/ICIOT.2018.00012.

[5] H. Chi, T. Aderibigbe and B. C. Granville, "A Framework for IoT Data Acquisition and Forensics Analysis," 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 5142-5146, doi: 10.1109/BigData.2018.8622019.

[6] Chhabra, G. S., Singh, lVarinder P. and Singh, M. (2018) ‘Cyber forensics framework for big data analytics in IoT environment using machine learning’, Multimedia Tools and Applications, pp. 1–20. doi: 10.1007/s11042-018-6338-1.

[7] Al-Masri, E., Bai, Y. and Li, J. (2018) ‘A Fog-Based Digital Forensics Investigation Framework for IoT Systems’, in 2018 IEEE International Conference on Smart Cloud (SmartCloud), pp. 196–201.

[8] V. R. Kebande et al., "Towards an Integrated Digital Forensic Investigation Framework for an IoT-Based Ecosystem," 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), Xi'an, 2018, pp. 93-98, doi: 10.1109/SmartIoT.2018.00-19.

[9] Babun, L., Sikder, A.K., Acar, A., & Uluagac, A.S. (2018). IoTDots: A Digital Forensics Framework for Smart Environments. ArXiv, abs/1809.00745.

[10] Qatawneh, Mohammad & Almobaideen, Wesam & Alkhanafseh, Mohammed & Qatawneh, Ibrahim & Al,. (2019). DFIM: A NEW DIGITAL FORENSICS INVESTIGATION MODEL FOR INTERNET OF THINGS. 24.

[11] S. Sathwara, N. Dutta and E. Pricop, "IoT Forensic A digital investigation framework for IoT systems," 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 2018, pp. 1-4, doi: 10.1109/ECAI.2018.8679017.

[12] Conti, Mauro & Dehghantanha, Ali & Franke, Katrin & Watson, Steve. (2017). Internet of Things Security and Forensics: Challenges and Opportunities. Future Generation Computer Systems. 78. 10.1016/j.future.2017.07.060.

[13] Islam, Md & Mahin, Md & Khatun, Ayesha & Roy, Shanto & Kabir, Sumaiya & Debnath, Biplab. (2019). A Comprehensive Data Security and Forensic Investigation Framework for Cloud-IoT Ecosystem. 4.

[14] Qatawneh, Mohammad & Almobaideen, Wesam & Alkhanafseh, Mohammed & Qatawneh, Ibrahim & Al,. (2019). DFIM: A NEW DIGITAL FORENSICS INVESTIGATION MODEL FOR INTERNET OF THINGS. 24.

[15] Hyunji Chung, Jungheum Park, Sangjin Lee, Digital forensic approaches for Amazon Alexa ecosystem, Digital Investigation, Volume 22, Supplement,2017,Pages S15-S25,ISSN 1742-2876,https://doi.org/10.1016/j.diin.2017.06.010.

[16] Islam, Md & Mahin, Md & Khatun, Ayesha & Debnath, Biplab & Kabir, Sumaiya. (2019). Digital Forensic Investigation Framework for Internet of Things (IoT): A Comprehensive Approach. 10.13140/RG.2.2.11356.03205.

[17] Karabiyik, Umit & Akkaya, Kemal. (2019). Digital Forensics for IoT and WSNs. 10.1007/978-3-319-92384-0_6.

[18] Hossain, Mahmud & Karim, Yasser & Hasan, Ragib. (2018). FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger. 33-40. 10.1109/ICIOT.2018.00012.

[19] T. Bakhshi, "Forensic of Things: Revisiting Digital Forensic Investigations in Internet of Things," 2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST), Karachi, Pakistan, 2019, pp. 1-8, doi: 10.1109/ICEEST48626.2019.8981675.

[20] J. Hou, Y. Li, J. Yu and W. Shi, "A Survey on Digital Forensics in Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 1, pp. 1-15, Jan. 2020, doi: 10.1109/JIOT.2019.2940713.

[21] Alabdulsalam, Saad & Schaefer, Kevin & Kechadi, Tahar & Le-Khac, Nhien-An. (2018). Internet of things forensics: Challenges and Case Study.

[22] Rizal, Randi & Hikmatyar, Missi. (2019). Investigation Internet of Things (IoT) Device using Integrated Digital Forensics Investigation Framework (IDFIF). Journal of Physics: Conference Series. 1179. 012140. 10.1088/1742-6596/1179/1/012140.

[23] Alenezi, Ahmed & Atlam, Hany & Alsagri, Reem & Alassafi, Madini & Wills, Gary. (2019). IoT Forensics: A State-of-the-Art Review, Challenges and Future Directions. 10.5220/0007905401060115.

[24] Shah, Anal & Rajdev, Palak & Kotak, Jaidip. (2019). Memory Forensic Analysis of MQTT Devices.

[25] Anthraper, Joseph & Kotak, Jaidip. (2019). Security, Privacy and Forensic Concern of MQTT Protocol. SSRN Electronic Journal. 10.2139/ssrn.3355193.

[26] Koroniotis, Nickolaos & Moustafa, Nour & Sitnikova, Elena & Slay, Jill. (2017). Towards Developing Network forensic mechanism for Botnet Activities in the IoT based on Machine Learning Techniques.