Objective:-

IoT crime is a main challenge which is a combination of major technology areas such as mobile devices, cloud computing, tablets, computers, RFID technologies and sensors. IoT forensics [1] is used to obtain the evidence which is in the form of digital from IoT devices for a legal purpose. The digital evidence on IoT is divided into three groups:-

a) Forensics collected from sensors and smart devices;

b) Forensics from hardware and software which are included in the traditional way that providesaninteraction betweenexternal world (e.g., computers,IPS, IDS, mobile and firewalls) and the smart devices, which are included in traditional computer forensics; and

c) Evidence collected outside the network from hardware and software under investigation. This includes social networks, cloud, mobile network providers, ISPs and internet.

Background/Literature Review:-

The Internet of Things is a physical object in networks which is accessed through internet. It makes our daily lives more dynamic and convenient but on the other side, it creates an opportunity for the hackers and other security and privacy issues which impact the peoples directly. The IoT allows the interaction between human-to-things, things-to-things and human-to-human. It is also a concept of enabling the communication between intelligent machines. By the name, you can guess that it converts the data from several kinds of objects or things to any dynamic platform which exists in an Internet infrastructure [2].In 1982, the concept of IoT is introduced when a machine of coke reports the drinks contained whether it is cold or warmand all these will be done through the internet [3]. Later, in 1991, Mark Weiser gave a vision of IoT, in the form of ubicomp where it is made to appear everywhere and anytime [4]. However, in 1999, A Device to Device communication is developed by Bill Joy.In the same year, the term “IOT (Internet of Things)” was proposed by Kevin Ashton to describe a system of interconnected devices [5]. IoT is a thought of interconnectivity which describes a world that anything will be connected and communicated in a quick fashion. It has the ability to track and code the objects which allows companies to make the processes easier, prevent theft, reduce error, provide security,

become more efficient and incorporate flexible and complex organizational systems through IoT. Further, IoT models and architectures are introduced by several authors, researchers and practitioners to provide security which helps to reduce the risk while transmitting through internet. To resolve the security issues IOT manufacturers adopted IoT device certification standard to release software updates in the way of automatic patching. The researchers Asim&Iqbal andBaccelli, Peterson &Tsiftes (2016) [6] found a common OS for IoT environment such as RIOT, FreeRTOS, Mbed and Contiki. The interaction between IoT and objects will be possible through the software and get enabled through the OS along with the RFID and WSN technologies. The OS for IoT has few unique security features like stability and usability. Also, it occupies only few kilobytes of memory and use low power consumption. It was quite different from other operating systems by providing security in terms of encryption, data hiding techniques and intrusion detection. It still prones the third party attacks to protect IoT infrastructures.Internet of Things was inspired by RFID community members who identified the possibility of object that can be tagged through radio waves like serial number by browsing through an internet address.The IoThas some key technologies such as sensor technology, RFID,and intelligence embedded technology. The IoT enables the users to bring physical objects into the cyber world by usingdifferent tagging technologies like RFID, NFC and 2D barcode which allows the physical objects to get identified and referred over the internet.RFID device is very helpful for identifying friend or foe which was used in 2nd world war in Brittan in 1948. Later, in MIT, the technology is founded at Auto-ID center in the year 1999. The project called GITAR (Generic Extension for IOT Architectures) which was discussed by Lin and Bergmann in 2016 [7] is used to create a software patching on regular basis which means system update. It is similar to Microsoft windows update except it would integrate GITAR into different IoT OS on closing off the security risks or vulnerabilities by the updates before a breach occurs. Recent growth in the IoT industry helps IoT manufacturers across the industries to update and upgrade the softwares. The sensors patching and devices makes the device manufacturers to reduce security risks for all IoT devices.

Research Methods:-

The research will be conducted in three phases:

- **Extensive review of literature concerning IoT:** The literature review helps us to understand that IOT has become integral part of cyber security in recent times. The functioning of IOT has gone beyond the

native meaning of just connecting two devices. The extensive literature review let us understand that with IOT multiple other technologies have also developed side by side to provide a better assistant to the security. This includes mechanical intelligence, automatic patching, sensors and more. A insight on IOT also helps us understand that forensic science which was previously based on testing and methodology has come across a long way with the usage IOT, which has made research and resolving of issues relatively easier.

- **Extensive review of literature concerning IoT and embedded forensics:** The literature review helps us understand how IOT has helped in development and advancement of tools used by forensics for their research and resolving of cases. The literature review helps us understand the digital hardware model and its implication in forensics in resolving issues. Some of the embedded hardware that helped in forensic like JTAgulator, TEKpro, Triplett 1101B and more has been actively because of introduction of IOT.
- **Identification and comparison of current methods and techniques as they apply to IoT forensics:** Forensics in today's world is completely based on IOT however, the methods of research that IOT forensics use are derivation of the old way of research with usage of technology to make the functioning and work easier. The methodology of forensic IOT has to go through the following steps:
- Identification
- Preparation
- Approach strategy
- Preservation
- Collection
- Examination
- Analysis
- Presentation
- Evidence returning

References:-

1. Oriwoh, E., Jazani, D., Epiphaniou, G., &Sant, P. (2013). Internet of Things Forensics: Challenges and Approaches. Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing. doi:10.4108/icst.collaboratecom.2013.254159.
2. Ling-yuanZeng, "A Security Framework for Internet of Things Based on 4G Communication," in Computer Science and Network Technology (ICCSNT), 2012, pp. 1715-1718
3. The "Only CokeMachineontheInternet,"CarnegieMellon University, School of Computer Science.
4. M. Weiser, "The computer for the 21st century", Sci. Amer., 1991, pp.66-75.
5. Kevin Ashton, "ThatInternetofThings," RFIDJournal, 22 June 2009.
6. Asim, M., &Iqbal, W. (2016). IoT operating systems and security challenges. International Journal of Computer Science and Information Security, 14(7), 314-318.
7. Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. Information, 7(3), 44.doi:http://dx.doi.org.ezproxy1.apus.edu/10.3390/info703004.