Asian Journal of Engineering and Applied Technology
ISSN: 2249-068X (P) Vol.11 No.1, 2022, pp.14-20

DOI: https://doi.org/10.51983/ajeat-2022.11.1.3304

Security and Privacy Concerns for the Modern Technology of Internet of Things

Samiya Majid Baba and Indu Bala
Department of Electronics and Communication Engineering, Lovely Professional University, Punjab, India
E-mail: samiyababa165@gmail.com, indu.23298@lpu.co.in

(Received 11 January 2022; Accepted 3 February 2022; Available online 10 February 2022)

***Abstract* - The Internet of Things (IoT) is present in every aspect of our lives. They are used in our households, in hospitals, and outside to monitor and report environmental improvements, deter fires, and perform a variety of other useful functions. However, both of these advantages can come at the expense of significant security and risks privacy. Several academic research have been conducted to counteract these issues and figure out a better way to remove or minimise the threats to the user's privacy and protection specifications in IoT devices. The survey is divided into four parts. The first section would look at the most important shortcomings of IoT devices and how to overcome them. The description of IoT attacks will be presented in the second section. The final section would look at security problems at various layers.**
***Keywords:* Internet of Things (IoT), Security, Privacy, Technology**

I. INTRODUCTION

Internet of Things (IoT) is a set of things/products/systems that are equipped by various sensors, actuators and microcontrollers that are linked to the Internet in order to gather and share information. Sensors and computing power are built into IoT applications, allowing them to be used in a variety of settings. The lack of a human role distinguishes the Internet of Things from the conventional Internet. IoT devices can collect data on people's habits, interpret it, and take action based on it. While the services offered by IoT applications are beneficial to human life, they can come at a high cost in terms of privacy and security safety. Security analysts have warned of the possible danger of vast quantities of unsecured computers connected to the Internet when IoT vendors neglected to incorporate a comprehensive security mechanism in the devices.

The first IoT botnet was discovered in December 2013 by a researcher at Proof point, an enterprise security agency. According to Proof point, gadgets other than computers make up more than 25% of the botnet, counting TV, child monitoring & various different home gadgets. Dyn, a domain name service provider based in Manchester, New Hampshire, encountered service outages recently as a result of what appeared to be a well-coordinated attack. Multiple websites, including Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, Sound Cloud, and The New York Times, were made inaccessible to users on October 21st, 2016, due to a distributed denial of service (DDoS) attack leveraging an IoT network of user machines.

IoT applications keep on presenting huge security and protection issues for clients, as they bring an unheard of degree of online protection concerns. This is due to the fact that these machines don't accumulate individual information, for example, names of customers and telephone numbers, however they can also follow their commitment for instance, when clients are at home and what they had for lunch. Many users are vigilant of storing a sensitive data in clouds as a result there is a never-ending series of massive data leaks, and for good cause. Several surveys have been conducted on security issues and various challenges have been released.

Granjal *et al.,* [1] looked at current implementations for IoT structured networking protocols (PHY, MAC, Network, and Application) as well as cross-layer structures when necessary. Sicari *et al.,* [2] discussed research problems and existing strategies in the field of IoT protection, with an emphasis on the seven major security issues: authentication, access management, confidentiality, anonymity, trust, protected middleware, mobile security, and policy compliance. They brought up some unresolved questions and offered some suggestions for potential analysis. The analysis of clustered and dispersed methods was the subject of Roman *et al.,* [3]. They presented an attacker model that could be used in both clustered and hierarchical IoT architectures, as well as a look at the key problems and promising solutions in security mechanism design and implementation.

In this survey paper, we look at four different areas of IoT protection and privacy. The first section discusses the most important shortcomings of IoT devices as well as potential alternatives. The second section delves into the description of current IoT attacks. Finally, we look at security problems and processes in the vision, network, transport, and device layers, in that order.

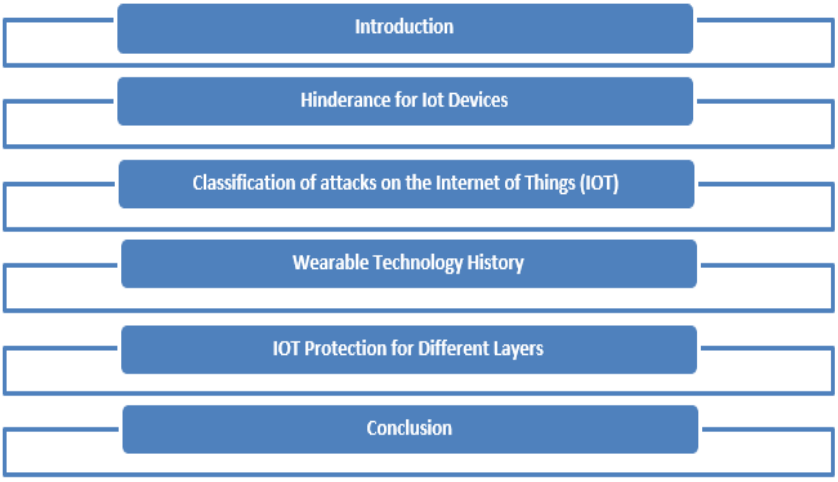

Fig. 1 Flowchart of the Research paper

II. HINDRANCE FOR IOT DEVICES

Trappe *et al.,* [4] discussed IoT restrictions and how they affect the use of existing cryptographic tools, such as those used on the conventional Internet. The battery size and computing power are the two major constraints.

A. Prolonging the Life of the Battery

Since certain Internet of things gadgets are used in locations where there is no possibility of charging, they have a limited amount of energy power to perform the intended functions, and serious protection orders will deplete the devices' power. There are three options for dealing with this problem. The first one is to utilize the device's minimum security specifications, which is not a good idea, particularly when working with confidential information. The second choice is to boost battery power. Most IoT computers, on the other hand, are built to be compact and compact. There isn't sufficient space for a larger battery. The last alternative is to extricate power from regular assets (e.g., sun, fire, friction contact, and wind waves), yet this will require an innovation update and significantly raise the monetary expense.

B. Easy Computation

According to the one paper, traditional cryptography cannot be used on IoT systems because the devices' memory capacity is insufficient to accommodate the computational and storage needs of sophisticated cryptography algorithms. The authors proposed reusing current functions to enable protection protocols for restricted applications. Physical layer verification, for example, can be used to check if a communication originated from the intended originator in the normal position by using signal processing on the receiver side. Alternatively, a transmitter's basic analogue characteristics can be used to accurately encode analogue data. These analogue complexities are impossible to anticipate or monitor in production, and they may serve as a one-of-a-kind key. Since radio signals are used, this method of authentication has a low to no energy overhead. For the Internet of Things, Shafagh *et al.,* [5] suggested "an Encrypted Query Processing algorithm". The method allows for the safe storage of encrypted IoT data in the cloud, as well as the effective processing of database queries over encrypted data. They utilize Elliptic Curve El Gamal and impermanent request safeguarding encoding calculations, which they adjusted to meet the processing restrictions of IoT PCs.

The structure conspire replaces web worker availability with an End-to-End framework that keeps up scrambled information from PCs on a Cloud network and performs information encryption and decoding at the customer. The keying material would just be put away on the client's PC, eliminating the need for a trustworthy proxy with access to all of the hidden keys. Three key players make up the system architecture: IoT computers, user individual, and the Cloud. The application data may be directly uploaded to the Cloud via the smart device or by a proxy, such as a wearable device. The paper just looked at a few encryption mechanisms that serve the most popular IoT data processing queries. The concept, on the other hand, can be expanded to accommodate more schemes. When compared to current systems, the experiment findings showed an increase in time efficiency.

Kotamsetty *et al.,* [6] suggested a method for reducing latency for IoT during database processing over encrypted data by using a strategy called latency hiding, which involves breaking down large query results into smaller data sets. This helps you to do cryptographic work on a collection of information at the same time as retrieving the left over encrypted data information. The study suggested an algorithm that begins actually with the size of an initial data plus adjusts it adaptively to minimise the difference between computation and contact latencies in each iteration in order to minimise latency. The algorithm comes in two flavours: the first begins with a smaller scale than the large question size. The starting size is set in the second version. The discoveries of the examinations showed that the

proposed strategy beats current techniques regarding inertness for inquiries of more noteworthy informational indexes. Salami *et al.,* [7] recommended a stateful Identity-based Encryption-based lightweight encryption plot for shrewd homes, in which the public keys are basically character strings and no computerized testament is required. The stateful IBE conspire set up by Phong, Matsuka, and Ogata (PMO) is recognised as Phong, Matsuka, and Ogata (PMO). It's Diffie-Hellman (DH) encryption plot that consolidates IBE and stateful Diffie-Hellman (IBE). The examination study recognizes the encryption technique into key encryption and information encryption, with an accentuation on the last mentioned, since the measure of cipher texts created by key encryption is more prominent than that delivered by information encryption. This expands the unwavering quality of the proposed plot and lessens transmission costs. Because of this detachment, two sub-calculations arose: KEY Encrypt and DATA Encrypt. The first is utilized to scramble a meeting key, while the second is utilized to encode subtleties. The subsequent cipher text from the sub calculations is sent independently, so information cipher texts are sent a few times without the fundamental cipher text. The discoveries of the test uncovered that the proposed framework is protected from plaintext attacks. Likewise, the presentation audit uncovered that it outflanks the standard IBE conspire as far as accelerating encryption tasks and lessening transmission overhead by around a third.

C. Classification of Attacks on the Internet of Things (IoT)

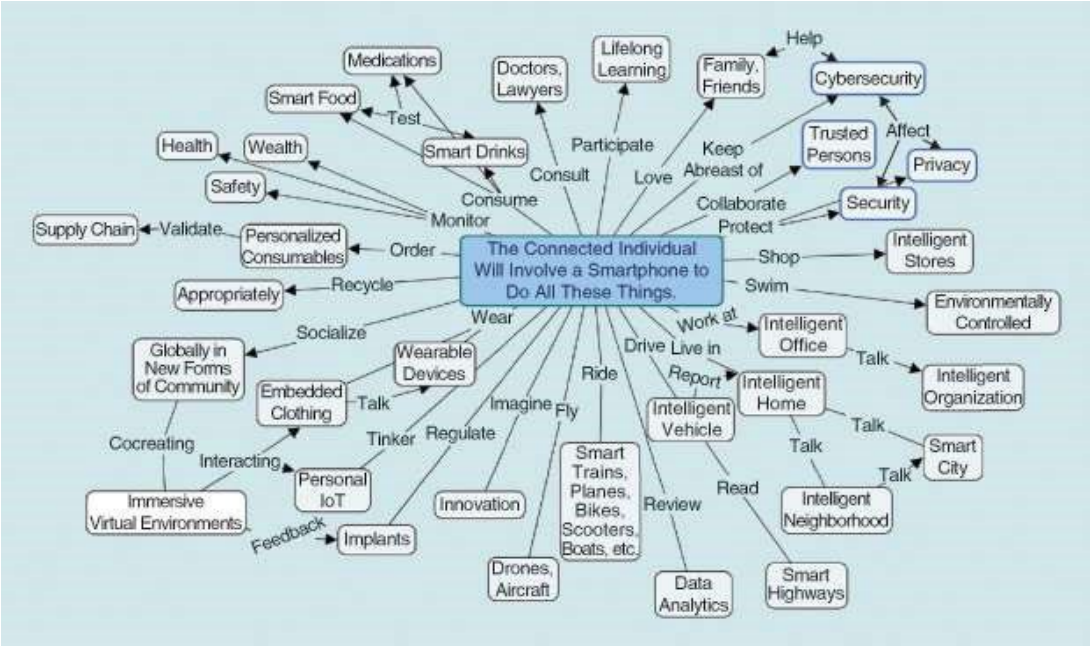

Fig. 2 A brainstorm of what it will be expected from a Smartphone to do for a user

IoT defence has been the focus of considerable study in the past. They've separated Internet of Things attacks and solutions into helpful groups. Andrea et al. [8] suggest another significance of IoT system attacks, which they orchestrate into four groupings: physical attack, network attack, application, and cryptography attacks and one covers a substitute layer of the Internet of Things structure (physical, network, and application), just as information encryption IoT conventions. At the point when the interloper is inside nearness to the PC, an actual attack is completed. The network attack incorporates incurring interruption to the IoT network framework by controlling it that cause harm to the framework.

Programming attacks emerge where IoT frameworks have security bugs that cause an assailant to exploit the circumstance and harm the gadget. Encryption attacks are endeavours to unscramble the framework's encryption. Man in the middle attacks, Side channel, Cryptanalysis, and are for the most part instances of this sort of attack. They likewise showed diverse security strategies for managing Internet of Things structure layers, encryption gadget bugs, and security issues. As indicated by the report, to limit assurance worries at the physical layer, the framework should utilize safe booting, which includes using cryptographic hash calculations and advanced marks to approve validation and programming trustworthiness. Before any information transfer or receipt, a new framework needs to approve itself to the network.

A PC ought to likewise have a deficiency acknowledgment highlight and data of the framework ought to be encoded to guarantee information security and mystery. Validation conventions and start to finish encryption at the network layer may be used to ensure information security and launching dependability. Notwithstanding hostile antivirus protection, the application layer can give assurance through verification, encryption, and dependability checking, that only allows for the valid client to gain access to the information data via firewalls and via control records.

Ronen *et al.,* [9] proposed a novel terminology for Internet of Things attacks that mostly centred on how the attackers credits shift from those of legitimate Internet of things items. The styles are disregarding, diminishing, misusing, and growing the framework's abilities. The exploration was shone on assaults on keen lights with improved capacities. The principle attack included setting up a concealed channel to take arranged information from a structure that had shrewd lights connected to a delicate interior network, as per the report. A similar report utilizes an optical beneficiary that can peruse information from a distance of in excess of hundred meters by estimating the exact length and recurrence of little varieties in light power. The following attack exhibited how an assailant could utilize such lights to make strobes at delicate light frequencies, possibly uncovering their area. The tests uncovered that security issues should be focused on in the plan, execution, and coordination periods of IoT frameworks.

D. Wearable Technology History

TABLE I WEARABLE TECH TIMELINE

Year	Device
1975	Pulsar Calculator Watch
1979	Sony Walkman
1984	Casio Databank CD-40
1987	Digital Hearing Aid
1993	Apple Newton PDA
1999	First Blackberry
2000	First Bluetooth Headset
2001	Apple iPod
2003	Viatron C-Series
2004	Motorola Razr
2004	Gopro Camera
2006	Nike+iPod Kit
2007	Apple iPhone
2008	Fitbit
2011	Jawbone UP
2012	Nike Fuelband
2012	Pebble Watch
2013	Nissan Nismo Smart Watch
2013	Misfit Shine
2013	Google Glass
2013	Samsung Galaxy Gear

III. IOT PROTECTION FOR DIFFERENT LAYERS

The incorporation of the imagined situations in IoT contexts will be made easier by applying current Internet protocols to smart devices. Traditional Internet protocols' protection frameworks, on the other hand, must be changed or expanded to support IoT applications. We'll talk about security issues and current solutions in various layers of IoT systems in this section.

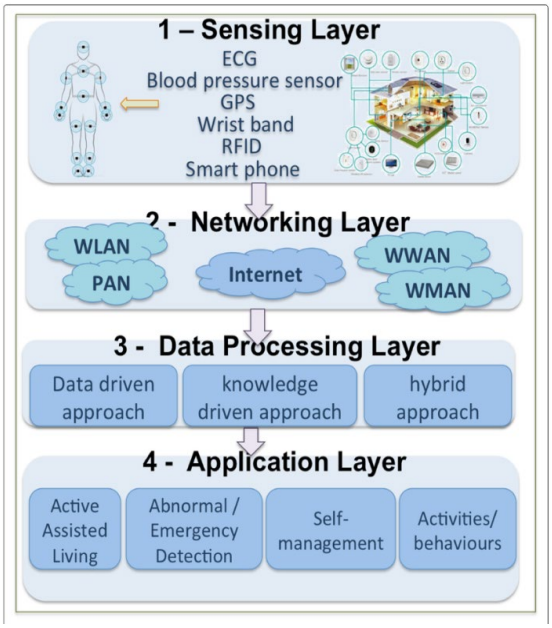

Fig. 3 Architecture for healthcare IoT based system

A. Perception Layer Protection in the Internet of Things

IoT is a device that collects and exchanges data from the real world. As a consequence, the physical layer comprises various sensors like temperature/ pressure/ humidity sensors, sound sensors, IR sensors, heart rate sensor, vibration sensors, motion sensors, and other forms of gathering and regulating modules. The two components of the perception layer are perception node that includes controllers and sensor and then second one is perception network that is connected with the transportation network [10]. The perception network leads the collected information to the gateway or leads control instructions to the dispatcher, and the perception node is used for data collection and data control. Wireless sensor networks (WSNs), implantable medical devices (IMDs), Radio-Frequency Identification (RFID), and the Global Positioning System (GPS) are examples of awareness layer technologies.

The identification of suspicious sensor nodes is one protection problem in the perception layer. This will happen if a node is physically attacked (e.g., killed, disabled) or if it is intruded/compromise by cyber-attacks. In general, these nodes are referred to as defective nodes. It is important to be able to identify unreliable nodes and take steps to prevent further loss of service in order to ensure service efficiency. To recognise defective nodes in Wireless sensor network, Chen *et al.,* [10] suggested and tested a localised fault detection algorithm. For the Wireless sensor network, Silva *et al.,* [11] suggested a model of a decentralised intrusion detection system. Wang *et al.,* calculated the interruption recognition prospect in both homogeneous and heterogeneous WSN.

The cryptographic algorithms & key control system to be used are another security issue for the perception layer. For

node authentication, the public key algorithm has been found to be useful. It is more flexible and can help protect the whole network without needing a complex key management protocol. Three low-power public key encryption algorithms, according to Gaubatz *et al.,* [12], are the most promising candidates for wireless sensor networks: Rabin's Scheme, NtruEncrypt, and Elliptic Curve Cryptography. Hidden key generation, delivery, preservation, upgrading, and degradation are all part of key management. There are four types of primary delivery systems currently in use: (1) Transmitted key distribution, second one is the distribution of grouped, third one is the pre distribution of the master key and the fourth one is the pair wise key distribution.

When uploading confidential data to the collection server, some IoT users are concerned about their privacy. It's essential to encrypt information prior to submitting it consequently the receiver can't identify the submitter. Many recent studies have looked at anonymous data aggregation. Yao *et al.,* [13] recently suggested an effective encrypted data collecting protocol for sensing in the interactive IoT applications in a recent article. A stage for reserving a slot and a stage for submitting a message make up the protocol. In the stage of a reserving a slot, total number of n users gives information or message in a vector slot that serves as a stage for reserving a time slot and another for sending a post in a hidden form from the rest of the group and the aggregator. During the message accommodation point, every client sends encoded information to the aggregator dependent on opening data that is simply known to her, and the aggregator can't associate the information got to a specific client. The recommended information revealing convention breaks the connection between the gathered information and the donor, protecting client security.

IMDs are an advanced type of Internet of Things gadget that is inserted inside the human form for demonstrative and restorative uses. It is authoritative to guarantee the security of IMDs on the grounds that even a minor defect will put a patient's life in risk. However, numerous attacks have been demonstrated in recent years to be capable of effectively compromising a variety of commercial IMD devices.

The vulnerabilities of a commercial implantable cardioverter defibrillator were presented by Halperin et al (ICD) [14]. They were able to figure out the ICD's informing convention and acquire the patient's and ICD's own subtleties using an oscilloscope and a device radio. They have performed active attacks in order to modify the treatment settings & void the battery quicker. Snooping and dynamic attacks, on the other hand, will disrupt commercial glucose control and insulin delivery systems. They had the option to mimic the specialist and change the normal treatment by replaying and infusing messages with a product radio after figuring out the contact convention and packet design. Barnaby Jack, a technology expert, has also discovered major security bugs in IMDs and shown how an attacker can remotely manipulate an insulin pump, pacemaker, or ICD. Security accidents and flaws in IMD goods should be the responsibility of the IMD producers. They are, however, reluctant to integrate robust protection features into their goods because these improvements would incur increased monetary costs and reduce the product's operating existence.

In 2014, a free security scientist named Billy Rios discovered 100 imperfections in the PCA 3 Life care mixture siphon's interchanges framework, which was fabricated by the clinical gadget partnership Hospira (HSP). These bugs cause a programmer to acquire admittance to the siphons and change the volume of medication that is intended to be administered. Rios reached Hospira, however the firm didn't react. Hospira stayed calm on the matter until April 2015 [15], when another analyst, Jeremy Richards, openly uncovered the danger. The US Food and Drug Administration (FDA) and the Department of Homeland Security (DHS Industrial)'s Control Systems Cyber Emergency Response Team at that point sent warnings to clinics notice them about the risks of Hospira siphons and encouraging them to change to substitute implantation frameworks [16]. Numerous advancement exercises have been given to IMD access the board and asset corruption assault avoidance.

B. Network Layer Protection in the Internet of Things

To permit IPSec correspondence with IPv6 hubs, it is worthwhile to extend IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) for IoT gadgets in a WSN sense. This is valuable since current Internet end-focuses should not be refreshed to interface securely with the Wireless sensor network, and authentic end-to-end encryption can be upheld without the utilization of a steady passage. Start to finish (E2E) safe correspondence between IP fuelled sensor organizations and the traditional Internet was recommended by Raza *et al.,* [17]. They went over the particulars of the Encapsulating Security Payload (ESP) for 6LoWPAN/IPSec and contrasted it with the generally utilized 802.15.4 connection layer security. The 6LoWPAN/IPSec approach and 802.15.4 insurance were tried on a hearty testbed, which reuses the crypto equipment utilized in current IEEE 802.15.4 handsets for 6LoWPAN/IPSec.

Granjal *et al.,* proposed a cutting edge secure interconnection model and assurance components to take into consideration start to finish security and the consistent mix of IP permitted WSNs with the Internet. 6LoWPAN protection headers are executed in their model to allow beginning to end security between sensor centres, similarly as frameworks to explicitly screen the energy proceeded with security methodology on the WSN.

Jara *et al.,* [18] assessed the standards and wanted usefulness for IoT versatility uphold and recommended a savvy approach zeroed in on Mobile IPv6 and IPSec for confined conditions. The reasonableness of Mobile IPv6

and IPSec for confined gadgets was investigated, and a lightweight form of Mobile IPv6 and IPSec was contemplated, arranged, created, and assessed. The proposed lightweight Mobile IPv6 with IPSec arrangement knows about IoT details and gives the best answer for complex conditions as far as execution and steadiness, which is modified to the capacities of IoT-gadgets.

C. Transport Layer Protection in the Internet of Things

Considering existing Internet standards, particularly the DTLS show, Kothmayr *et al.,* [19] offered the primary totally executed two-way verification arrangement for the IoT structure. The proposed scheme depends on the trading of X.509 testaments containing RSA keys during a completely confirmed DTLS handshake. It can associate with 6LoWPANs utilizing standard correspondence stacks that help UDP/IPv6 organizing. For DTLS, Raza *et al.,* [20] proposed 6LoWPAN header pressure by using standardized steps as they associated stuffed DTLS to the 6LoW-PAN standard. The proposed DTLS pressure diminishes the amount of additional security bits by a critical sum. For instance, the quantity of extra security bits in the DTLS Record header, which is added to each DTLS packet, can be diminished by 62%. In their subsequent work, they propose Lithe, an IoT coordination of DTLS and CoAP.

They additionally proposed another DTLS header compression scheme that utilizes the 6LoWPAN norm to essentially lessen energy utilization. Because the 6LoWPAN Border Router does not typically perform any approval, Brachmann *et al.,* [21] tried to point out that security features like Transport Layer Security (TLS) or DTLS using Internet do not actually imply that equivalent levels of security can be fine-tuned in the Low-power and Lossy Network (LLN), that is currently unsecured against consumption of resources, flooding, replay, and improvement attacks. The creators proposed two systems for countering those kinds of assaults. The underlying advance is to plot the TLS to DTLS convention show at the application layer to guarantee start to finish security. To ensure the LLN, the subsequent methodology is to utilize a DTLS-DTLS burrow.

Hummen *et al.,* [22] examined the "utilization of declarations for the companion verification in the field of Web of things". For the authentication based DTLS handshake, fundamental overhead assessments are performed. The creators proposed three plan thoughts dependent on pre-approval, meeting resumption, and handshake designation to diminish the overheads of the DTLS handshake.

D. Application Layer Protection in the Internet of Things

Smart home (e.g., learning indoor regulator, keen and smart bulb), clinical and medical services (e.g., ongoing wellbeing checking framework), smart city (e.g., brilliant lighting, parking system), energy consumption (e.g., powerful networks, powerful metering), natural observing (e.g., environment observing, untamed life following), mechanical web, and associated vehicles are only a couple instances of IoT applications. Most of present day IoT gadgets have programmable embedded PC frameworks. Some are even full-fledgedly fit for running complex programming and similar like useful PCs, putting them at risk of the same security threats. They may become infected by computer viruses such as trojan when connected to the Internet.

The Internet of Things (IoT) is allowing malware to be utilized to make incredible botnets in a new environment. Mirai, a recently a piece of Linux malware has been discovered to be utilized to oppress IoT gadgets. Mirai can acquire shell access by utilizing the telnet or SSH records' default passwords. It can make postponed measures, erase documents, and even introduce other malware on the framework whenever it has accessed the record. The infected devices were secretly controlled by Mirai and were waiting for orders to launch a DDoS attack. A DDoS attack utilizing compromised IoT gadgets running the Mirai malware caused a massive internet outage in October 2016.

Thereafter, Malware Must Die security researchers found another malware family called IRCTelnet, which is furthermore planned to debase Linux-based unsteady Internet of Things (IoT) devices and change them into a botnet for massive DDoS assaults. IRCTelnet, as Mirai malware, relies upon default hard-coded passwords. By savage obliging Telnet ports and debasing the contraption's working structure, it arranges an IoT device. The IoT gadget in this way transforms into a botnet combat room that can be controlled through Internet Relay Chat (IRC), an application layer convention that considers text-based correspondence. DDoS attacks in the IoT and WSN have been widely explored.

IV. CONCLUSION

In this paper, we have addressed the privacy and security problems in Internet of things devices and in different application of IoT. We addressed solutions for extending the battery life and easy computing, as well as the drawbacks of IoT devices in terms of battery and computing power. We also looked at current approaches for classifying different IoT attacks and discussed the security mechanisms. The final section of our paper looked at security and safety problems and their solutions from four perspectives that is: Generally, the security of industrial IoT devices is determined by the innovations, conventions, and security processes used by each producer. Depending on the situation, all Internets of things devices can be vulnerable to specific attacks. This highlights the importance of establishing a broad collection of security policies and set of guidelines for Internet of Things devices. To combat newly emerging threats and establish solid and stable security guidelines for Internet of thing gadgets and systems, the IoT's manufacturing industry must cooperate closely with supervisory agencies.

REFERENCES

[1] J. Granjal, E. Monteiro, and J. S. Silva, "A secure interconnection model for ipv6 enabled wireless sensor networks," in *IFIP Wireless Days*, pp. 1-6, Oct. 2010.

[2] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, Vol. 76, pp. 146-164, 2015.

[3] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, towards a Science of Cyber Security Security and Identity Architecture for the Future Internet, Vol. 57, No. 10, pp. 2266-2279, 2013.

[4] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the internet of things," *IEEE Security Privacy*, Vol. 13, No. 1, pp. 14-21, Jan. 2015.

[5] H. Shafagh, A. Hithnawi, A. Droescher, S. Duquennoy, and W. Hu, "Poster: Towards encrypted query processing for the internet of things," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '15, New York, NY, USA: ACM, pp. 251-253, 2015.

[6] R. Kotamsetty and M. Govindarasu, "Adaptive latency-aware query processing on encrypted data for the internet of things," in *25th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1-7, Aug. 2016.

[7] S. A. Salami, J. Baek, K. Salah, and E. Damiani, "Lightweight encryption for smart home," in *2016 11th International Conference on Availability, Reliability and Security (ARES)*, pp. 382-388, Aug. 2016.

[8] I. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in *IEEE Symposium on Computers and Communication (ISCC)*, pp. 180-187, July 2015.

[9] E. Ronen and A. Shamir, "Extended functionality attacks on IoT devices: The case of smart lights," in *IEEE European Symposium on Security and Privacy (Euro S & P)*, pp. 3-12, March 2016.

[10] J. Chen, S. Kher, and A. Somani, "Distributed fault detection of wireless sensor networks," in *Proceedings of the 2006 Workshop on Dependability Issues in Wireless AdHoc Networks and Sensor Networks*, ser. DIWANS '06, pp. 65-72, 2006.

[11] A. P. R. daSilva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in *Proceedings of the 1st ACM International Workshop on Quality of Service & Amp; Security in Wireless and Mobile Networks*, ser. Q2SWinet '05, pp. 16-23, 2005.

[12] G. Gaubatz, J. P. Kaps, E. Ozturk, and B. Sunar, "State of the art in ultra-low power public key cryptography for wireless sensor networks," in *Third IEEE International Conference on Pervasive Computing and Communications Workshops*, pp. 146-150, March 2005.

[13] Y. Yao, L. T. Yang, and N. N. Xiong, "Anonymity-based privacy-preserving data reporting for participatory sensing," *IEEE Internet of Things Journal*, Oct. 2015.

[14] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *IEEE S&P*, 2008.

[15] David Goldman, "A hacker can give you a fatal overdose," [Online] Available: http://money.cnn.com/2015/06/10/technology/drug-pump-hack/, 2013.

[16] FDA, "Two safety communications on the cyber security vulnerabilities of two hospira infusion pump systems," [Online] Available: http://www.fda.gov/MedicalDevices/Safety/Alertsand Notices/default.htm, 2015.

[17] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, and U. Roedig, "Securing communication in 6lowpan with compressed ipsec," in *2011 International Conference on Distributed Computing in Sensor Systems and Workshops(DCOSS)*, pp. 1-8, June2011.

[18] A. J. Jara, D. Fernandez, P. Lopez, M. A. Zamora, and A. F. Skarmeta, "Lightweight mipv6 with ipsec support," in *Mobile Information Systems*, 2014.

[19] T. Kothmayr, C. Schmitt, W. Hu, M. Bryunig, and G. Carle, "Dtls based security and two-way authentication for the internet of things," *Ad Hoc Netw.*, Vol. 11, No. 8, pp. 2710-2723, Nov. 2013.

[20] S. Raza, D. Trabalza, and T. Voigt, "Blowpan compressed dtls for coap," in *2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems*, pp. 287-289, May 2012.

[21] M. Brachmann, S. L. Keoh, O. G. Morchon, and S. S. Kumar, "End-to- end transport security in the ip-based internet of things," in *2012 21st International Conference on Computer Communications and Networks (ICCCN)*, pp. 1-5, July 2012.

[22] R. Hummen, J. H. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, "Towards viable certificate-based authentication for the internet of things," in *Proceedings of the 2Nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy*, ser. HotWiSec '13, pp. 37-42, 2013.