A new approach to secure internet of things(IoT) devices using encryption and anonymity capabilities of The Onion Router (TOR)

[1] Skanda Kumar.B, [2] Nandan goud.B
[1] Ballari Institute Of Technology and Management, Karnataka ,India.
[2] Nandi high school, Ballari, Karnataka, India.

***Abstract:* - A new revolution of the Internet is the Internet of things (IoT) where various devices and systems are connected to leverage data anywhere, anytime that is expected to spread rapidly, over the coming years.it is estimated that IOT is beneficial for smart home devices as nearly 40 billion connected devices are expected to be in use by 2020 but the biggest problem with such it devices is with limited functionalities is the security. Securing communications between devices and their back-end systems is one of the most severe problems. In some specific IoT cases, VPN can handle the secure connection, but VPN is not always possible. Hence there Is an immediate need for better technologies and innovative methods through which the hot network security can be greatly enhanced by using The Onion Router(TOR). By default, all traffic in the Tor network is encrypted and the identities and locations of traffic sources are very effectively concealed. Thanks to this, someone intercepting traffic from Tor networks is neither able to identify the sender nor view or alter the messages. These features would be useful when securing an IoT system. Tor network is commonly considered only something which is criminal. in this paper the author is trying to look TOR objectively which is perfectly legal and show its positives uses like securing IoT devices preventing any future catastrophic large-scale cyber attacks.**

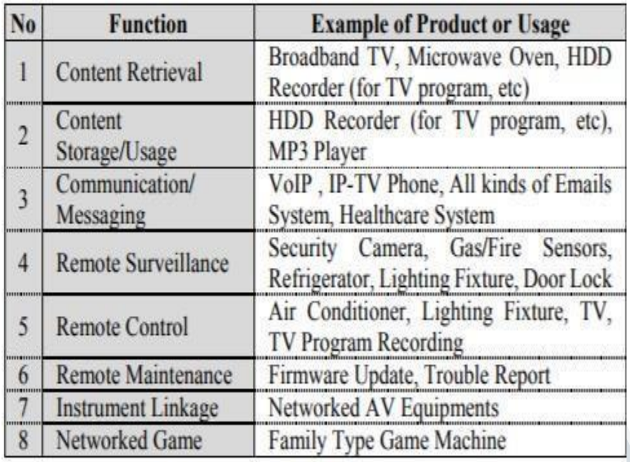
Keywords— TOR; Security; Internet; Network ;IoT; Anonymous communication.

I. INTRODUCTION

Nowadays, thanks to the impressive achievement of material science especially in semiconductor equipment and nanomaterials, all the electronic devices are getting smaller in size, and microprocessors can be found in most appliances. Such developments have been leading mankind a newera of technology[2,3], the era of the “Internet of Things”(hereafter: IOT), where all the appliances are getting tiny and controllable via the Internet[3,4], thus enabling people to enjoy network-based services, such as Video on Demand (VOD), Music on Demand (MOD), remote update, ecommerce, remote control, and other similar services. Digital information has become social infrastructure and with the expansion of the Internet, network infrastructure has become an indispensable part of social life and industrial activity for mankind. The idea of using existing electronics in smart home appliances and connecting them to the Internet is a new dimension along which technologies continue to grow, and inrecent years mankind has witnessed an up surge of usage of devices such as smart phone, smart- television, home health-care device, smart LED light bulbs system, etc. Theirbuild-in internet-controlled function has made them quite attractive to man segments of consumers and smart phone ha become a common gadget for social networking. There are, however, serious challenges which need to be addressed as these tiny devices are designed for specific functions and lack processing capacity required for most security software. Furthermore, researchers around the world have come up with an abundance of clever ideas on how to effectively use microprocessors and Internet in other everyday household appliances. ‘Smart’ has become the new buzzword that we have kept on hearing in recent years, for example, in ‘smart ‘homes, ‘smart’ kitchens, ‘smart’ ovens, ‘smart’ refrigerators etc. Table (1) indicates the functional classification of smart home appliances. There is a so a tremendous business potential for them because of foreseen future demand[9] older adults, where the number of people over the age of 65 is expected to double to 70 million by 2030. According to toa study conducted by International Data Corporation, 212billion “things” will be installed based on IoT with an estimated market value of

$8.9 trillion in 2020 [9]. Those“things” will be nothing special but daily used appliances ranging from a watch, light bulb to smart television, refrigerator and so on.

Tabe 1: Functional classification of smart home appliances



No	Function	Example of Product or Usage
1	Content Retrieval	Broadband TV, Microwave Oven, HDD Recorder (for TV program, etc)
2	Content Storage/Usage	HDD Recorder (for TV program, etc), MP3 Player
3	Communication/ Messaging	VoIP , IP-TV Phone, All kinds of Emails System, Healthcare System
4	Remote Surveillance	Security Camera, Gas/Fire Sensors, Refrigerator, Lighting Fixture, Door Lock
5	Remote Control	Air Conditioner, Lighting Fixture, TV, TV Program Recording
6	Remote Maintenance	Firmware Update, Trouble Report
7	Instrument Linkage	Networked AV Equipments
8	Networked Game	Family Type Game Machine

Dark Web and the Tor network is typically considered only something criminal. But if we take an objective look, it can offer positive uses as well. One such use could be more secure IoT networking. Dark Web comes out to be a surprising solution to secure IoT. Anything unknown is often considered a threat. For instance, in the Game of Thrones series people called “wildings” were first seen just as hostile barbarians. Later, they became a valuable ally for Jon Snow, one of the most prominent characters. If we think of the world of networks, Tor is one such unknown, as its famous nickname Dark Web shows. Commonly, Tor is thought of as a service used to access something dangerous and illegal, such as sites selling drugs or stolen identities. While there is some truth in this, it only covers a fraction of possible and real uses. The Tor network can be utilized for useful and legal purposes as well. Remember, Tor was originally not created for or by the bad guys. It originated from the necessity of providing secure communications for dissidents. Securing connections in IoT. Anonymous communication on the Internet seems finally within reach. Though an initial commercial deployment of Onion Routing The Freedom Network, was in the end shut down, a volunteer-run replacement network using the second-generation onion routing design Tor has been operational for several years and had about a thousand nodes and a hundred thousand users Tor is used by an increasing variety of parties: reporters communicating with sources, dissidents and embassies hiding their activities from local governments , people trying to get around geographic restrictions and more.[1,2]

II. BACKGROUND

Tor is a popular privacy enhancing system that is designed to protect the privacy of Internet users from traffic analysis attacks launched by a non-global adversary. Because Tor provides an anonymity service on top of TCP while maintaining relatively low latency and high throughput, it is ideal for interactive applications such as web browsing, file sharing, and instant messaging. Since its initial development, researchers have analysed the system’s performance and security[5] properties. Before moving in to detailed technical demonstrations, it is necessary to briefly introduce some important properties of TOR. In the previous research we already described its internal working mechanism and showed that it is indeed an ideal anonymous communication tool which employs asymmetric cryptography, takes advantage of public-key encryption and transmits data from a source to a destination through a randomly selected route of multiple nodes [4]. Raw data having its destination IP address encrypted Andre-encrypted with public key of the selected nodes, something which resembles an onion ring where in each layer is a re-encrypted version of an encrypted data by the public key of the node. In the transmission process, each node decrypts a layer of the encryption to extract the next layer’s IP address, an operation resembling an onion-peeling-off process. The final node decrypts the last layer of the encryption and sends the original data to its real destination without revealing or even knowing its original sender [1]Tor’s system architecture attempts to provide a high degree of anonymity and strict performance standards simultaneously [1,2,5]. At present, Tor provides an anonymity layer for TCP by carefully constructing a three-hop path (by default), or circuit, through the network of Tor routers using a layered encryption Shining Light in Dark Places: Understanding the Tor Network 65 strategy similar to onion routing [1,2]. Routing information is distributed by a set of authoritative directory servers. In general, all of a particular client’s TCP connections are tunnelled through a single circuit, which rotates over time. There are typically three hops in a circuit; the first node in the circuit is known as the entrance Tor router, the central node is called the middle Tor router, and the final hop in the circuit is referred to as the exit Tor router. It is important to note that only the entrance router can directly observe the originator of a particular request through the Tor network. Also, only the exit node can directly examine the decrypted payload and learn the final destination server. It is infeasible for a single Tor router to infer the identities of both the initiating client and the destination server.

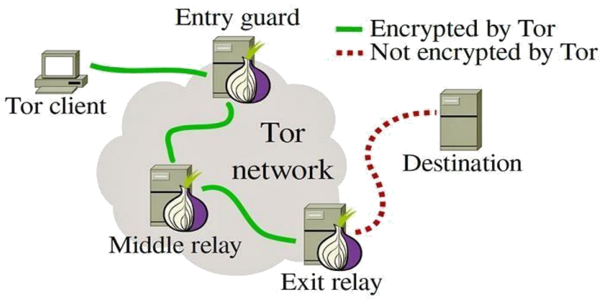


Figure 1: working of Tor network

To achieve its low-latency objective, Tor does not explicitly re-order or delay packets within the network. The Internet of Things (IoT) is expanding rapidly, with projections of 50 billion connected devices by 2020 [2,3]. These devices will provide an unprecedented ability to sense and control our environments, from our homes through our utilities our industries, in our cars and on our bodies. Sensor data can be aggregated across our devices and sent to remote data centres to be analysed. Device control can be initiated from across the world. Industrial equipment makers are routinely adding sensors and network connectivity to equipment such as turbines that have traditionally been controlled only locally to yield cost savings due to increased monitoring and remote control [5]. The positive potential of connected devices and analytics is driving significant investments into the IoT, the Industrial Internet and Machine-2-Machine communications. One promising application of IoT is in our homes. Smart-home technologies provide sensors and controllers throughout our homes that promise energy savings, home automation, and other cost savings and conveniences.in the below part of the paper an effort will be made to show how these two technologies can be integrated to create a secure network for the internet of things.

III. MAIN THRUST OF THE PAPER

Connecting smart home appliances to the Internet, however, makes us vulnerable to malicious attacks. An intruder can steal private information such as contact info, shopping or eating preferences, lifestyle and relaxation habits, or credit card information used to pay for such services. They can also use smart appliances as launching pads to carry out malicious attacks into other systems To secure IoT devices over a TOR network the well-known regular Tor hidden service shall not be used as it just merely turn your IoT devices of smart home into a normal Tor hidden service, which are usually designed to allow anyone access to a website while routing the traffic over Tor's network of thousands of volunteer computers to prevent visitors from knowing where the computer that hosts the site is physically located. Instead, the better way to secure the IoT devices of the smart home system would be to use a lesser-known feature of Tor called an authenticated secret service. By using this service, the Tor's intermediary computers can't connect to the destination computer at all without the user implementing a particular passcode .this method makes the network of IoT devices, not just anonymous but secures the IoT devices to an extent wherein even the voluntary computers cannot hack into the IT network.Taking into consideration all of the aforementioned cyber attack cases aimed at smart appliances, it is apparent that the attack techniques are not new. However, what have been changed are the attack targets, which are the smart home appliances and devices in IoT network. In most cases, the attackers make complete use of the nature of Internet Protocol to have access to those data services; and often, the devices do not have full-functional display or screen, so it is tough for the victims even to detect that they are being attacked and abused internally. Furthermore, different from human-controlled computers, most of the smart appliances (such as LED light bulbs smart system, smart refrigerators, and smart meters) can easily be accessed due to their 24 hours around-the-clock availability on the Internet. Last but not least, because each appliance is designed to serve only a particular purpose, marketability factors such as low cost, portability, tinier size, etc. make built-in full cryptography capability infeasible in most of such appliances. There have already been experiments of this idea The Guardian Project, a Tor Project contributor[8], has developed a way to keep the army of devices from toasters and refrigerators to lawn sprinklers and HVAC systems, from rising up at the behest of hackers and spilling sensitive data or executing other cyber attacks[8], by integrating Tor security into the Internet of Things. Working with Home Assistant, an open source platform built on Python, Guardian Project[1,8] Director Nathan Freitas was able to create the "Tor Onion Service Configuration" for the scalable system. The platform, which runs on devices including Raspberry Pi, can control and network IoT. Too many 'Things' in our homes, at our hospitals, in our businesses, and throughout our lives are exposed to the public Internet without the ability to protect their communication. Tor provides this, for free, with realworld hardened, open-source software and strong, state of the art cryptography," Tor can provide secure remote access to your Home Assistant instance as an Onion site, through Tor's Hidden Service feature. With this enabled, you do not need to open your firewall ports or setup HTTPS [2]to enable secure remote access[7,8].This is useful if you want to have the Access your Home Assistant instance remotely without opening a firewall port or setting up a VPN and Don't want to or know how to get an SSL/TLS certificate and HTTPS configuration setup and in need and Want to block attackers from even being able to access/scan your port and server at all want to block anyone from knowing your home IP address and seeing your traffic to your Home Assistant

Figure 2 : TOR and IOT working together

IV. FUTURE TRENDS

All the top five emerging domains IoT, cloud, mobile application, artificial intelligence, Big data can exploit and take reap uses with the running on TOR network to enhance the security as all of the domains face the threat of being a victim of cyber attack.In the near future almost 40 billion connected devices are expected to be in use by 2020, and NFC provides a simple solution for connecting IoT devices to a network and hence there is greater need for improving the TOR network at the first place there is enormous scope to do more research on developing TOR network and further research can also be made by utilising the network simulator (NS3)software wherein individual packets can be traced ;by using network simulating large software scale it projects like smart cities and integrated smart home over a tor network can be analysed, and further research can be done by publishing the experimental results.

V. CONCLUSION

By connecting all devices to internet forming not have large number of applications as in future by 2020 nearly 30 billion devices would be connected to internet A decade ago it was impossible internet of things a reality, Since the Internet of Things is still at the early stage of its development, smart home appliance producers need more time and effort in order to produce cost-effective and safe products. Until then, however, being aware of cyberattacks aimed at smart home appliances and its numerous risks, having an alternate solution to remedy the potential problems is quite important. but in just past five years and with the same acceptance of IOT by 2020 there is scope of IOT due to huge number of devices that will be connected to internet but dream can be made into a reality once people gain trust over it, this can be only be done by creating more secure internet for it devises to get connected .to sum up, using seemingly suspicious Dark Web technology could significantly reduce the security risks related to networking IoT devices. Now and then, clearing our heads of unnecessary prejudices can pay off. Tor could be something unknown and threaten that in the end becomes our ally.

REFERENCES

[1] ITheTor Project, "Tor: Documentation", Torproject.org, 2017. [Online]. Available: https : // www.torproject. Org /docs /documentation.html.e n.

[2]D. McCoy, K. Bauer, D. Grunwald, T. Kohno and D. Sicker, "Shining Light in Dark Places: Understanding the Tor Network", Privacy Enhancing Technologies, pp. 63-76.

[3]Atzori, L., Iera, A. and Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), pp.2787-2805.

[4] B. Borowicz, "Simplifying IoT: Connecting, Commissioning, and Controlling with Near Field Communication (NFC) - Grid Connect Blog," Grid Connect Blog, 2017.

[5] M. Schurgot, D. Shinberg and L. Greenwald, "Experiments with security and privacy in IoT networks", 2015 IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015.

[6] M. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker and H. Chen, "Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT)", 2014 IEEE Joint Intelligence and Security Informatics Conference, 2014.

[7] A. Chaabane, P. Manils and M. Kaafar, "Digging into Anonymous Traffic: A Deep Analysis of the Tor Anonymizing Network", 2010 Fourth International Conference on Network and System Security, 2010.

[8] A. Greenberg, A. Greenberg, L. Newman, L. Newman, A. Greenberg, B. Barrett, A. Greenberg and C. Bozelko, "Now You Can Hide Your Smart Home on the Darknet", WIRED, 2017.

[9] Carrie MacGillivray, Vernon Turner, Denise Lund, Worldwide Internet of Things (IoT) 2013–2020 Forecast: Billions of Things, Trillions of Dollars. International Data Corporation, 2014. Available:

VI. ACKNOWLEDGEMENT

The authors wish to thank the management and staff of Ballari Institute Of Technology and Management, Karnataka, India for the support and The authors would also want to thank Nandan Goud B who is just 15 years old for contributing to ideas.

Bio-data

Skanda Kumar B is pursuing the bachelor of engineering 3rd year , a student from Ballari Institute Of Technology and Management, Karnataka, India. His research and learning areas include emerging domains like IOT, cloud, mobile application, artificial intelligence, Big-data and several basic sciences fields like quantum physics genetic engineering and atomic structures and is looking forward to pursue masters in computer science after undergraduation

Nandan goud .B is studying in 10th grade , Nandi high school, Ballari, Karnataka, India. He has a keen interest in various topics in computer sciencelike artificial intelligence ,mobile applications, basic science, chemistry, etc. and is looking forward to completing his under graduation IIT's