

Web of Things: Security Challenges and Ways

Waman Sujit S.¹ Prof. Rokade M.D.²

^{1,2}Department of Computer Engineering

^{1,2}Sharadchandra Pawar College of Engineering, Dumberwadi, Omer, Maharashtra, India

Abstract— Web of things (WoT) is an advanced and highly promising internet of things (IoT) allows smart devices to not only connect to the internet but also the web. Allows users to share content creation and provide data integration and analysis skills through a network to be part of the World Wide Web (W3). Despite these developments, it has shown some security challenges that need to be addressed in order to successfully use WoT in commercial transformation as well large scale. In this paper, the authors analyze the most significant security challenges associated with such WoT such as unauthorized access, listening, and denial of service attacks, outbursts, and impersonations, through analysis of applied studies that have already been published. In addition, we have discussed some of the options available to overcome security-related issues while considering network size and mobility. The writers did used to analyze Threats and attack modes to inform users about preventive measures and this prevent security threats from using system errors Authors provide the necessary understanding on how security can be improved using specific methods and algorithms. Findings by research reveals that safety measures to protect WoT are still maturing and future research is needed to solve these challenges.

Keywords: Web of things (WoT), Internet of Things (IoT), World Wide Web (W3)

I. INTRODUCTION

In this modern age, the internet is very much connected things in the global network and in this network, the web provides a universal platform for resource sharing, archiving and publishing services, etc. In WoT “things” refers to tangible or intangible objects and “web” refers to these objects accessible through web services, such as HTTP and APIs text can be used in protocols and service layers respectively to embed intelligent and intelligent realities also WoT is expected to make access to smart devices easier and promote the integration of novel resources for web services in the physical world (sensors, electronics, and intelligence)

It gives us exciting skills to change the in the world and add quality to our lives just as the web does 20 years ago. Relationship between WoT and IoT is just like the relationship between the web and the Internet. WoT is supported by IoT in the network layer intended to provide any device such as phones, laptops, An integrated editor that integrates reviews of this manuscript once authorizing its publication was Qing Yang. Routers, computers, and more with an IP address. At that point, WoT means IoT in the application layer with intended for the provision of electronic devices such as QR, Bluetooth, beacons, etc. by URL. The web of things can be defined as to expand current and evolving strategies through web tools and provide the development of IoT conditions for to facilitate the creation of IoT applications. By removing all complexity and several transport contracts after IoT, WoT offers the advantage to the developer to focus only in their programs without worrying

about devices as well protocols are active. OSI (open systems interconnection) has a seven-layer structure to establish multiple levels and network protocols. Similarly, WoT buildings have four layers namely; access layer, sharing layer, composition layer and availability layer, cluster editing of web tools and policies become an important framework for connect anything or things to the web. The main purpose design WoT Architecture to accelerate the installation of smart devices and services available web and assist in the implementation of web applications called using intelligent objects the structures are not solidly designed and concealed especially from the previous layers. Instead, architecture should be considered a multi-faceted project a network which is a step by step, which makes implementation easier of applications that use smart devices. WoT design provides services address every layer needed to look smart as top web citizens. However, applications can be integrated at the top of the appropriate layer provided for implementation of service or more of their integration depending on special application. But, combining apps with using smart features in their intuitive OS (operating system), libraries and agreements still need some skills as well. The purpose of all WoT building forums is the foundation for that bringing this development to the attention of the hobbyist and the web developers with technical knowledge and thereafter brings I development and implementation of nearby IoT applications for end users by allowing them to create simple applications tailored to their needs. Several new web-based technologies such as semantic web, service-focused web, cloud computing, IoT and WoT making the cyber world a hot topic for researchers only but also a global network of cooperation and cooperation places where many organizations, communities and organizations are formed. The cyber world in the social world it always grows. The pioneer concept of communication real-world objects on the World Wide Web began about 2000. But in 2002, the authors proposed a cool city project in linking material to web pages for information and connected services. Both IoT and WoT ideas see the world there communication can be made anywhere and anytime but these ideas cannot be edited in the real world without dealing with important factors such as trust, security, and privacy. Wise things include almost every aspect of our daily lives. The number of devices connected to WoT is growing clearly. In 2015, 15.41 billion devices were connected on the web and by 2025 is expected to have 75.44 billion devices will be connected to. Unfortunately managing security and privacy on these connected devices is a major challenge for four reasons features. The first factor is the heterogeneous type of the IoT because it contains an unlimited number of variables devices with different protocols, connections, and requirements. The second feature is inadequate resources such as IoT devices have limited resources available. The third factor is verification and identification. Typically, IDs were linked to people to see if they could perform a particular action or not. In the digital world and material things know the behavior of

both themselves and someone else. There is a need addressing ownership management issues and finding solutions securely manage property ownership and authorization process. So far many researchers have made their efforts investigate to identify management threats but nonetheless, shared the definition of object ownership does not exist. Fourth the feature is private as WoT is considered a highly connected system where information appears separately. .

II. RESEARCH CONTRIBUTIONS

The main contribution of this work is threefold: (a) Writers identify the main issues of the WoT in terms of term security; (b) Authors used analysis of threats and attacks modelling methods to inform users about preventive measures and preventing security threats from exploiting profits of system errors (c) In addition, the authors provide the required an understanding of how security can be improved through practice methods and algorithms.

III. LITERATURE REVIEW

IoT is a term used to build connections between different objects, systems, objects, people, or applications and WoTs Safety Challenges and Method PICTURE 2. Connected by a billion from 2015 to 2025.to control them from a web browser or mobile application. But, creating one social network that is trying connecting with multiple subjects is a challenge. I Semantic Web of Things is a current testing platform combining semantic web-based technologies with IoT. It can also be considered a change in the Web of Things (WoT) by adding semantics. SWOT directed ability exchanging and using information between data and ontology. However, WoT allows control of and access to IoT applications and services using standard web technologies such as JavaScript, PHP, or HTML 5.0. In WoT, any device can be accessed using standard web protocols. All this the three technologies include some security and privacy problems because, a large number of connected devices produce multiple scales, variations, and interactions news. At this stage, the authors have already reviewed studies published with a view to safety identification Challenges in WoT, SWoT, and IoT. WoT allows users to connect and share information. The social media web is also an emerging concept of WoT. The WoT-related privacy threats to privacy are discussed at all a layer of properties such as administration, acquisition, syncing, privacy, enclosed internet and understanding of WoT and IoT additional authors also proposed solutions for to overcome them. WoT integration with wireless sensor networks provides the ability to connect real-life objects with a combined system. While inclusive, serious issues have been raised over access to smart personal information related to smart personal belongings and privacy. The authors propose that it is possible to strengthen the security of the environment by using protective tools such as securities protocols, strictly constructed and well-tested codes, used encryption technology, and security testing over APIs. Web traffic logs, in the WOT area, provide valuable information about how people interact with smart things by web servers. These web access logs play an important role role in building application security management. Because for this purpose, the authors introduced an algorithm called request a dependency graph to

investigate the behavior of clients by graphing the relationship between HTTP requests to them access web applications. The writers did experiments on data collected on real-world IoT mobile networks and the results obtained show a high degree of accuracy which is shows that the reliance graph is a good tool for mining web usage. The rapid production of IoT technology could be the cause of weak IoT networks is severely compromised by privacy as well security threats. The authors point out some security risk by creating three different IoT operating conditions liability for leaking personal information, leakage of sensitive user information, and unauthorized performance uses standard cheap and available retail products and services. The results of the use cases showed that IoT privacy and security agreements are not well defined by manufacturers and consumers leading to anonymous tracking of user behavior and ownership if the devices are not built privately and data is not classified as sensitive. WoT Appearance is integrated with the semantic web technology for creating a vulnerable semantic web of things as well highlights gaps in the domain such as technical interaction, syntactical interaction, and semantic interaction. Also, the authors discuss important safety issues such as confidentiality, integrity, honesty, authenticity, availability, and authorization of WoT with IoT issues. Issues involving legal issues, privacy, and security order provide ownership among existing technologies outside the shelf provided in. Also, the researchers presented the bag research Inter Data Net, which is a framework for WoT and is used in the wise cities of Spain, Santander to use security solutions in real-time use to test them strengths and weaknesses. On IoT privacy issues, security, and trust in both information and devices is proposed in. In addition, abbreviated IoT-related security issues are being reviewed din by reviewing the safety structures and requirements of four layers of structures namely network layer, support background, visualization, and application background. The authors discussed three safety issues Layers of IoT Architecture i.e. application, vision, and the IoT transport and defense layer, presented various threats to IoT security such as confidentiality, accessibility, integrity, authenticity, and denial and discuss possible solutions to address these IoT threats effective use on a large scale in trade .Other important IoT challenges such as authentication, authorization, privacy, and integrity have been discussed of. Basic security principles and resource limits to ensure IoT is proposed in. This the study concluded that non-disclosure and liability exist possible in the IoT area of cybercrime in applications such as forensics, cyber-crime investigation, and much more R. Sardar, T. Anees: WoTs: Safety Challenges and Methods Overview of WoT .others. An in-depth analysis of IoT features such as autonomy, the spread, as well as the ubiquity of the universe have been discussed in.

IV. CONNECTING SOLID ITEMS ON THE WEB

There are two options for connecting smart devices to the web; indirect integration and direct integration. Household appliances can be viewed as direct integration and RFID can be viewed as indirect integration with the RFID reader and embedded server. Generally, the system can not only rely on one method but can use both integration methods as a

combination. A. DIRECT CONNECTION In order to integrate objects with the web, first of all things need to be configured as everything must have a single IP address when connected to the web. In the application layer, WoT also needs communication and collaboration. The web server must be embedded in such a way that businesses can communicate and interact with the web language defined by web principles. Most devices will work with IP and can be integrated with web services with the development of computer technology and communication technologies. Therefore, these devices can connect directly to other devices in any terminal with web browsers. Standard web functionality such as POST and GET can also interact with other devices. Developed a few smart web-based connectivity solutions. Sun SPOT powered by IP with a web server is introduced in. When each system in its image proposed its functionality on the web. In one proposed building, all small planning tools are integrated into the web, where sensor information and the use of sun SPOT are regularly displayed by web services. The prototype used for low-bandwidth Wi-Fi components to attach objects directly to the web is suggested. That model controls the interaction of HTTP protocols with IEEE 802.11 access points. B. INDIRECT CONNECTION All devices cannot be powerful enough to be integrated with web servers directly due to limited resources, such as RFID tags. Also, sometimes there is a need for smart devices to be directly connected to the web because of the power, security, and cost. In both cases, an indirect combination can be used. In this configuration, the central agent is located between the web and intelligent objects. This representative is called the wise gate. Wise things include a wise gate. Therefore, they will understand the special goals of intelligent things. A few solutions to indirectly integrate smart stuff with the web have been suggested. To enable the efficient query and manage the sensor network, the HTTP 1.1 protocol is used to embed the sensor gate. Smart sensor gates for intelligent network management and integration of sensor data designed by. In that paper the authors also built a Java applet to exchange data in a well-defined way. Other smart port implementation combinations of web-based and embedded device management are proposed in. The proposed gateway makes the sensor network accessible through a lightweight web service connection.

V. RESEARCH METHOD

The main purpose of this paper is to investigate security the challenges facing WoT have become threats not only in people's lives but also have damaged buildings. The process begins with a review of the current time WoT applications and officially update security Challenges facing WOT. Then he had an accident analysis and how to simulate the attack of a few security threats identified to detect system vulnerabilities. In addition, provide the proposed security already ways to improve these security challenges. In the end, provided a discussion section to discuss the findings of this study.

VI. APPLICATIONS

In modern times, WoT is used in many real-life applications. Experts always make good use of these: WoTs: Safety

Challenges and Method Research method. Technology to address the needs of the community. Variety WoT applications do wonders for this real world. Some researchers have used WoT and IoT in specific areas and different application domains that will be developed daily lives of At this stage after a brief review of WoT applications, the authors document the benefits and challenges of using WoT programs in Table 1. Combining IoT with WoT can offer a variety of benefits in the field of IT (Information Technology). Authors in used a combination of IoT and WoT in robots and encountered a variety of real-life examples such as sports, health, entertainment, culture, military, home support and surveillance, etc. through literature research for evaluation WoT conduct. The general idea is that variety Large WoT / IoT fields on robots are not touched by researchers at present. The authors in proposed a study of the WoT story in agriculture. Where they have developed an ontology that allows for architecture through a range of consistent natural sensors and different livestock monitoring methods to increase land efficiency. The authors in proposed WoT automotive connection structures using ITS-G5 data exchange between vehicles, processing, and storage units. WoT devices simplify and improve flexibility fidelity to infrastructure projects through compliance sensors, data analysis meters and lights for cost benefits and staff reductions and improvements urban security. Prior to WoT, waste management it was a big problem. Garbage containers can now be monitored to improve waste management and garbage collection route. The development of the Internet of Medicine has introduce major health care benefits such as management disease, remotely monitoring the patient's condition, treatment strategies and reducing costs and errors. This the change has had a profound impact on the health of patients and health workers alike. Also, some devices are smart to sensors can be used to monitor temperature regularly, heart rate, and other patient health conditions. It is also useful in homes where raw materials are used can be remotely controlled such as reducing water and electricity bills by monitoring energy and water meters. The rapid growth in the development of WoT machines worldwide has changed the daily lives of consumers. However, some security, privacy, general and legal matters they also appear for some reason. One of them is that a variety of products and vendors are available market and information about security as well the privacy of WoT machines is not readily available to them the user wants to consider it before purchasing. Author, reviewed security and privacy labels based on a series of surveys, interviews, users and help to 22 privacy and security experts and propose a prototype privacy and security labels to help consumers do the right thing decision before buying items. Another reason is that, smart devices transmit a lot the amount of wireless data in the cloud as a result WoT is facing more security challenges than ever before. There are many traditional ways to measure safety that should be protected WoT but these existing methods are not enough to deal with different types of attacks and their intensity. The authors in using machine and in-depth reading (DL) processes such as the neural network of deep, superstitious beliefs and unsupervised learning methods to improve safety methods in IoT, even in uncertain conditions.

VII. CONCLUSION

WoT transforms IoT as the web has transformed computers over the past decade. This communication prototype has we are employed in every aspect of our lives from intelligence cities in agriculture and industry but, communication between different devices create many security and trust issues. Thus, in this paper, major security issues such as these are highlighted such as unauthorized access, interference, impersonation, DoS, and configuration. An analysis of the threats was then used to mimic the attack on some of these highlighted threats security threats to detect potential system hazards it helps to protect the system from future attacks. In the midst of it all and issues, managing unauthorized access is considered a major issue threat to WoT connected devices. Protecting WoT connections between different devices also highlighted some of security measures such as access control, ownership management, confidentiality, and integration, authorization and verification. The authors used the Threat analysis and the attack model ways to inform users about preventive measures as well to prevent security threats from using the system errors. The authors provided the necessary understanding of how security can be improved by using certain available methods and algorithms. In our discovery, defense models are not yet mature yet further research is needed to ensure safety in WoT. In the author's view of ensuring safety, users' reliance on connected WoT devices can be achieved return returns major benefits such as reusable, easy access knowledge, and cost effectiveness. In the future, privacy and WoT-related issues of trust may be identified to make connections between different objects of nature easily.

REFERENCE

- [1] Ruhma Sardar, Tayyaba Anees. "Web of Things: Security Challenges and Mechanisms." Received January 22, 2021, accepted February 1, 2021, date of publication February 8, 2021, date of current version March 1, 2021.
- [2] Monika D.Rokade, Dr.Yogesh kumar Sharma,"Deep." IOSR Journal of Engineering (IOSR JEN), ISSN (e): 2250-3021, ISSN (p): 2278-8719
- [3] Monika D.Rokade, Dr.Yogesh kumar Sharma "MLIDS: A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset", 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), IEEE
- [4] Monika D.Rokade, Dr. Yogesh Kumar Sharma. (2020). Identification of Malicious Activity for Network Packet using Deep Learning. *International Journal of Advanced Science and Technology*, 29(9s), 2324 - 2331.
- [5] Sunil S.Khatal ,Dr.Yogesh kumar Sharma, "Health Care Patient Monitoring using IoT and Machine Learning.", IOSR Journal of Engineering (IOSR JEN), ISSN (e): 2250-3021, ISSN (p): 2278-8719
- [6] Sunil S.Khatal ,Dr.Yogesh kumar Sharma, "Data Hiding In Audio-Video Using Anti Forensics Technique For Authentication", IJSRDV4I50349, Volume: 4, Issue: 5
- [7] Sunil S.Khatal Dr. Yogesh Kumar Sharma. (2020). Analyzing the role of Heart Disease Prediction System using IoT and Machine Learning. *International Journal*

of Advanced Science and Technology, 29(9s), 2340 - 2346.