Internet of Things (IoT) Cybersecurity: A Study on Security and Privacy Threats, challenges and opportunities

Miss.Mashira Firdous, Prof.Arvind Kumar Pandey

MCA Final Year Student

Arka Jain University, Jamshedpur

Abstract:

As an emerging technology, the Internet of Things (IoT) changed the global network include of people, smart devices, intelligent objects, data, and informationIoT has an incredible opportunity to make the world a more elevated level of openness, trustworthiness, accessibility, classification, and interoperability. The main objective of IoT security is to preserve privacy, confidentiallythe advancement of IoT is as yet in its outset and many related issues should be settled.Ensure the security of the users, infrastructures, data, and devices of the IoT, and guarantee the availability of the services offered by an IoT ecosystem. With the help of IOT we can secure the global network even better.

Keywords:

Computer security, IOT, smart device, computer architecture, privacy, threats.

I. Introduction:

Internet of Things (IOT) is a prominent part of internet future. IOT has a infrastructure of network that is global where any object that is physically connected to internet has an identity and can communicate with the other devices on the internet. aThe gadgets like PCs, PDAs, tabs, clothes washers and so forth are a few to name. IOT is a huge network of interconnected ‘things’. The devices contain microchip that interconnects all the devices. These microchips track the surroundings and report the same in the network as well as to the humans. As a result of the low cost internet, huge number of devices ithe most awesome aspect of IOT is that every single actual substance can be imparted and is available through the web. connected to the internet.The quantity of gadgets associated with the web in 2008 was more than the people on the earthas per a think-tank, there were 4.48 billion gadgets associated with the web and the development in 2016 is required to be 30%. By 2020 it is relied upon to arrive at 50 billion.These devices result as a surface for attackers.The popularity of IoT or the Internet of Things has increased rapidly, as these technologies are used for various purposes, including communication, transportation, education, and business development. IoT introduced the hyper connectivity concept, which means organizations and individuals can communicate with each other from remote locations artlessly.About 26.66 billion IoT gadgets exist in the current world [1].The mass blast began in 2011 with the presentation of home mechanization, wearable gadget, and smart energy meters. The rapid explosion of IoT has benefittedthe unconscious use, not changing passwords, and the lack of device updates have increased cyber security risks and access to malicious applications to the IoT systems' sensitive data. Such unseemly security rehearses increment the odds of an information break and different dangers.Most of the security professionals consider IoT as the vulnerable point for cyber-attacks due to weak security protocols and policies. Despite the fact that few security components were created to shield IoT gadgets from digital assaults, security rules are not properly reported [2].Thereby, end-users could not utilize protective measures to avert data attacks. Programmers created various types of malware to contaminate the IoT gadgets since the night before 2008.

I. The IoT Concept:

The next revolution is expected to craft theinterconnection among diverse objects leading to what experts termed as the smart enludicrous decade; Internet advancements have upset the interconnection among individuals at an uncommon scale and speed ironmenAs we move from www (static pages web) to web2 (long range interpersonal communication web) to web3 (pervasive figuring—or web of things), the requirement for information on-request utilizing complex natural inquiries keeps on expanding altogether [2]. This era could be. named as the post-PC time where cell phones and related gadgets are changing our current circumstance and the way "things" (counting people) connect Things in the new environment are becoming more interactive as well as informative. Mark Weiser (father ofUbiquitous Computing), defined the new ecosystem as the ‘‘smart environment in theAs meactual world that is luxuriously and undetectably intertwined with sensors, actuators, shows, and
Computational components, installed flawlessly in the ordinary items, and associated through a ceaseless organization" [8].mentioned, Gubbi et al. [2] contended that the development of universal figuring are melded by distributed computing and the IoT. IoT as an idea is dared to have been begat by Kevin Ashton in an accommodation, where he contended "adding RFID and different sensors to regular items will make an Internet of Things, and establish the frameworks of another time of machine insight".

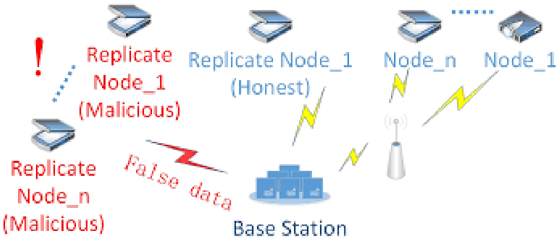
II. IOT TECHNOLOGIES AND SECURITY THREATS:

1. Physical Attacks

All the objects should have sensor to achieve its full capability. It is difficult to stop unauthorized physical access. A programmer can change hub/sensor information, along these lines the working of the entire sensor organization can be on hazard.

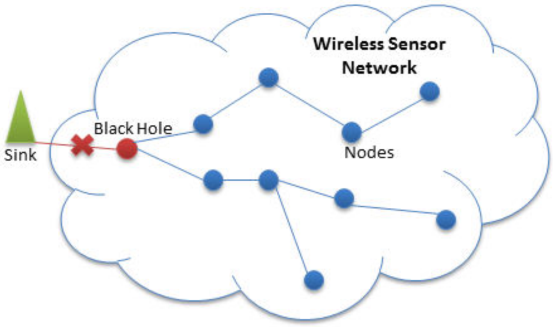
2. Node Replication

In this assault, a current hub id is duplicated to an organization with sensor.As a result of duplication of node packets are mis-routed, false sensor readings are recorded or a disconnection of network takes place. Thus, a sensor network's performance is disrupted.


!
Replicate Node_1 (Malicious)
Replicate Node_1 (Honest)
Node_n
Node_1
Replicate Node_n (Malicious)
False data
Base Station

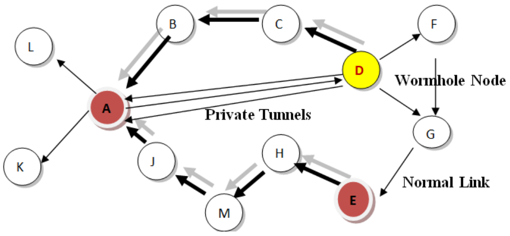
3. Selective Forwarding

In WSN, the nodes forward received messages to the destination. .A pernicious hub specifically advances parcels in this assault. Certain messages may be simply dropped without forwarding them. The modification of packets originating from few specific nodes is performed and the message is forwarded to the other nodes. Thus, it is difficult to identify the attacker.



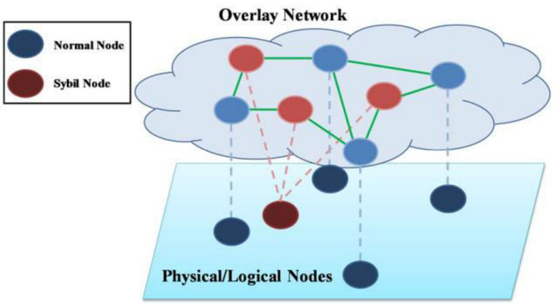
4. Wormhole Attack

It is a basic assault where the parcels is recorded at some area of organization and replays it to various area. This interaction can be completed specifically.



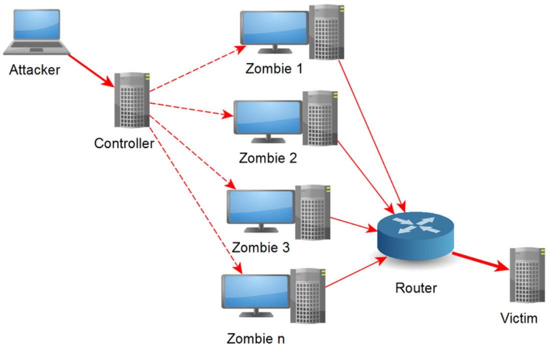
5. Sybil Attack

Sybil attack takes place when a computer is hijacked and the hacker claims multiple identities. In this attack, an adversary can manage to be at more than one place at one time. Here a single node presents multiple identities in the network which leads to significant reduction of effectiveness of fault tolerance.



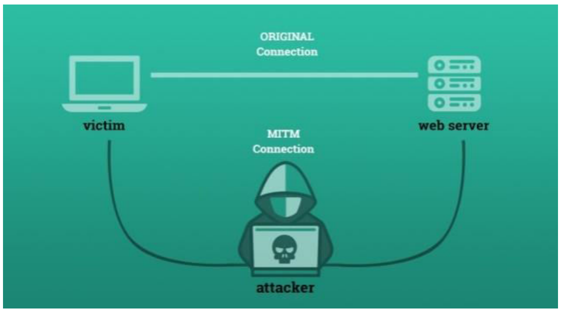
7. Service Attack denial

The services are made unavailable to legitimate users. Here, the connections of casualty are annihilated with legitimatelike demands from aggressor by flooding them. Subsequently, every one of the administrations are denied to the genuine clients.



8. Eavesdropping

In this assault, while the data is sent between the two hubs over the organization, the interloper tunes in to the data. Here, the data stays as before yet its security is undermined. This information can be used by the intruders against the users.



III. IoT Cybersecurity Challenges:

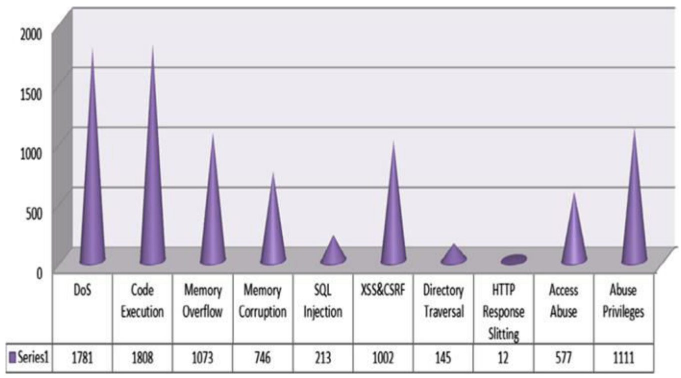
one key challenge which must be overcome in order to push IoT into the real world is security. Security challenges relating to IoT line up with the traditional Information Systems (IS) security objectives (SO) which are confidentiality, integrity, and data availability [12].

Moreover, there are other security challenges whichAppear to be IoT-specific. For instance, the converging of distributed computing and IoT, uncovered IoT stages to cloud actuated weaknesses, for example, those contained in OWASP top 10 [13].

These vulnerabilities which are inherent in cloudapplications are likely to impact on IoT solutions and services as the two emerge. Another huge danger vector might be found in unacceptable IoT items and administrations.These can possibly undermine the survivability of IoT administrations.For example, ineffectively planned, made and out-dated or fake items present extremely critical dangers to IoT empowered applications. Regarding this matter,

Furthermore, most IoT cyber security challenges lay in the system's own inherent vulnerabilities which expose the infrastructure setup to various attacks. The sources mayIncorporate firmware, equipment (gadget), framework applications, information, just as the organizationinterfaces or ports. Also, the bi-directional communication links between objects-to-objectsleave the system open for network-related attacks and protocol failure. Other related attacks include wireless scrambling, eavesdropping, man-in-the-middle attacks, and messagemodification and injection attacks. For example, IP-based devices are susceptible toIP misconfiguration which sometimes shows nondeterministic conduct regarding assault. IP misconfiguration unavoidably diminishes framework execution and dependability.

Additionally, while IoT and distributed computing reconciliation scales up IoT applications and administrations, the incorporation likewise uncovered IoT framework and reliant frameworks to Public organizations and worldwide passage. Notwithstanding IP caricaturing, administration entryways (both Neighbourhood and worldwide), can become ideal focuses for interruptions, Do's, infusion assaults and other Web/network-based assaults.Added to these, most IoT user interactive applications are web and/or mobile based, designed mostly with application programming interface (API) as the interface code architecture using PHP, Java, XML, and HTML. An unpatched API may be susceptible to various attacks exposing the entire system to malicious attacks.
For example, in CVE- 2016-7413, the ''use-after-free vulnerability in the wddx_stack_destroy function in ext./ wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service via a wddxPacket XML document that lacks an end-tag for a record setfield element, leading to mishandling in a wddx_deserialize call'' [13].Likewise, in CVE-2016-4539, "the xml_parse_into_struct work in ext/XML/xml.c in PHP before 5.5.35, 5.6.x, 5.6.21, 7.x and before 7.0.6 allows remote attackers to cause a denial of service (buffer under-read and segmentation fault) or possibly have unspecified other impact via crafted XML data in the second argument, leading to a parser level of zero'' [13]. In general, IoT systems are designed with security in mind, however, security misconfiguration can occur at any level of IoT communication architecture or any part of the system application.



IV. IoT Cyber Attack:

From the above challenges, we present a taxonomy of cybersecurity attacks on object-to objectcommunications by analysing system vulnerabilities vis-a`-vis potential threat actors.In this scientific categorization, six kinds of weaknesses are talked about.These are IP misconfiguration,injection, Do's, Code execution, Memory corruption, and XSS and CSRF.

V. Future Study and Scope:

Thread vectors incorporate physical (gadget) assault, application (programming) assault, organization assault, web interface assault, and information assault. Table 1 shows our proposed weakness danger network. In sections 3 and 4, danger vectors are coordinated with their comparing weaknesses.This paper will help to advance the scientific interests in the exploration of cybersecurity, particularly to respond to the procedural questions of the prediction of future data and actions significant to security patterns. This study sets the background to begin executing rules for all intentions as indicated through the usual security issues and answers for data systems. This paper consolidates many procedures connected and may be improved to serve cybersecurity regarding anticipating the operational legitimacy of the methodologies of assessment benchmarks. Finally, the emphasis on limiting, recouping, and disposing of weakness is the primary, basic patterns, and reactions to the constant expanding progress (Panchanatham, 2015).Over the next five years, cyber-crime may create severe damage in information technology. According to the researchers they have estimated an approximate close to 6 trillion dollars loss. So, there would be a very bright scope for people who work and resolve the issues related to cyber-crime and provide all the necessary security measures. Big organizations like CISCO which is completely related to networking technology which is one of the top organization has approximately millions of openings related to cybersecurity because which is the future for the safety of Information technology. They are also wide opportunities in government-related fields and also defence field to save the countries secure data from cyber attackers.

VI. Literature Review:

Sl.no	Title	Author	Finding	Remark
1.	IoT Device Security	Bendavid, Y.; Bagheri, N.;Safkhani, M.; Rostampour,	IoT design has novel security issues and associates with different layers, safety efforts ought to be considered for the whole engineering	In this study I got to know about the iotsecurity and different layes of safety.
2.	A Novel Algorithm for Detecting Sinkhole Attacks in WSNs	MalihehBahekmat, Mohammad Hossein Yaghmaee, Ashraf Sadat HeydariYazdi, and SanazSadeghi	The attacks to sensor networks can be considered from two Perspectives.Furthermore, these attacks, based on the capacities of the adversary, can be divided into two categories, named Mote and Laptop.	In this study I got to know about thewe need to utilize algorithms to obviate the security requirements of networks.
3.	Security Issues in Internet of Things	a.Balte, A., Kashid, &balaji Patil,	This implies that there are various challenges present while deploying IOT. The traditional security services are not directly applied on IOT due to different communication stacks and various standards.	In this study I got to know about the iot security challenges and the solutions.
4.	Integration of Cloud Computingand Internet of Things: a Survey	AlessioBotta, Walter de Donato, Valerio Persico, Antonio Pescap´e	IoT is fueled by the recent advances of a variety ofdevices and communication technologies, but things included in IoT are notonly complex devices such as mobile phones, but they also comprise every-day objects.	In this study I got to know thatCloud can offer an effective solution for IoT service management and composition as well as forimplementing applications and services.
5.	A Study Of Cyber Security Challenges And Its Emergning Trends On Latest Technologies	G.Nikhita Reddy1 , G.J.Ugander Reddy2	Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing.	It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

6.	A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments	Amandeep Singh Sohal, Rajinder Sandhu, Sandeep K. Sood	VHD is designed to store and maintain log repository of all identified malicious devices which assists the system to defend itself from any unknown attacks in the future.	cybersecurity framework is successful in identifying the malicious device as well as reducing the false IDS alarm rate.
7.	Blockchain mechanisms for IoT security	Denielminoli	Blockchains are powerful tools that well beyond basic security applications.	IoTblockchain approaches Fundamentally the IoT can utilize blockchains to ensure integrity of the business logic data.
8.	Internet of Things" Thing: In the Real World Things Matter More than Ideas	Ashton, K	develop an analytics engine which can gather sensor data from different devices and provide the ability to gain meaningful information from IoT data and act on it using machine learning algorithms.	Internet of Things middleware solutions that make the sensors and the actuators are able to connect to the Internet.
9.	On security challenges and open issues in Internet of Things	Sha, K.; Wei,W.; Yang, T.A.; Wang, Z.; Shi, W.	l IoT application is to build Smart Grid. Smart Grid has been designed and implemented to improve the reliability, reduce the cost, and optimize the performance of the traditional power grid systems	analyze security challenges resulted from the special characteristics of the IoT systems and the new features of the IoT applications.
10.	Deploying robust security in internet of things	Ruozhou Yu, GuoliangXue, Vishnu TejaKilari, Xiang Zhang	The unprotected and unmonitored transmission from IoT devices to the offloaded security mechanisms. An important challenge in modeling the security risk is the dynamic nature of IoT due to demand fluctuations and infrastructure instability.	In this study I got to know about robust deployment of security mechanisms in IoT.

VII. CONCLUSION:

Cyber-security is both about the insecurity made by and through this new space and about the practices or procedures to make it (progressively) secure.IoT has emerged as a significant technology. The data thatis transmitted from sensors or RFID tags may carry sensitiveinformation which must be protected from unauthorizedaccess. The IoT communication between two nodes is notsecure and the physical security of IoT devices should not becompromised. To achieve secure communication, IoT mustinclude services such as encryption, end-to-endenvironments,and access control for real-time and criticalinfrastructure protection. It is challenging in cybercrime tostay ahead of the attacker. In future, we can anticipate greater security for keen gadgets and the protection models of IoT correspondence will build which will permit the clients to robotize assignments helpfully utilizing this innovation .IoT with better security, information assurance methods and moral practices will unquestionably win client's trust and gain upper hand in the associated world.IoT cybersecurity technologies and cyber risk management frameworks.Then, this paper presented the four-layer IoT cyber risk management framework: the IoT cyberecosystem layer, the IoT cyber infrastructure layer, the IoT cyber risk assessment layer, and the IoT cyber performance layer.

VIII. REFERENCE:

1.Bahekmat, M., Yaghmaee, M. H., Yazdi, A. S., &Sadeghi, S. (2012). A Novel Algorithm for Detecting Sinkhole Attacks in WSNs. IJCTE, 4(3), 418-421.

2.Balte, A., Kashid, A., &Patil, B. (2015). Security Issues in Internet of Things (IoT): A Survey.International Journal of Advanced Research in Computer Science and Software Engineering, 5(4), 450-455. ISSN: 2277 128X.

3.Botta , A., de Donato, W., Persico, V. and Pescape, A., " Integration of Cloud computing and Internet of things: A Survey", Future Generation Computer Systems, Volume 56, March 2016, pp. 684- 700.

4.Gade, N. R., & Reddy, U. G. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies. Retrieved from https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies.

5. Sohal, A.S.; Sandhu, R.; Sood, S.K.; Chang, V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Comput. Secur. 2018, 74, 340–354. [CrossRef]

6. Yi, S.; Qin, Z.; Li, Q. Security and Privacy Issues of Fog Computing: A Survey. In Wireless Algorithms, Systems, and Applications, Proceedings of theWASA 2015, Qufu, China, 10–12 August 2015; Xu, K., Zhu, H., Eds.; Springer: Cham, Switzerland, 2015; Volume 9204, pp. 685–695.

7. Minoli, D.; Occhiogrosso, B. Blockchain mechanisms for IoT security. Internet Things 2018, 1, 1–13. [CrossRef]

8. Darianian, M., & Michael, M. P. (2008) Smart home mobile RFID-based Internet-of-Things systems and services. In International conference on advanced computer theory and engineering, 2008. ICACTE'08 (pp. 116–120).

9. Ashton, K. (2009). That 'Internet of Things' thing. RFID Journal, 22, 97–114

10. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279.

11. Bendavid, Y.; Bagheri, N.; Safkhani, M.; Rostampour, S. IoT Device Security: Challenging "A Lightweight RFID Mutual Authentication Protocol Based on Physical Unclonable Function". Sensors 2018, 18, 4444. [CrossRef]

12. Sha, K.; Wei,W.; Yang, T.A.; Wang, Z.; Shi, W. On security challenges and open issues in Internet of Things. Future Gener. Comput. Syst. 2018, 83, 326–337. [CrossRef]

13. Yu, R.; Xue, G.; Kilari, V.T.; Zhang, X. Deploying Robust Security in Internet of Things. In Proceedings of the2018 IEEE Conference on Communications and Network Security (CNS), Beijing, China, 30 May–1 June 2018;pp. 1–9. [CrossRef]Future Internet 2020, 12, 157 18 of 21