iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** V **Month of publication:** May 2021

DOI: https://doi.org/10.22214/ijraset.2021.34024

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue V May 2021- Available at www.ijraset.com

Future with the Internet of Things: Is it Secure or not?

Yash Mittal[1], Riya Jain[2], Suman Madan[3]
[1, 2]*Research Scholar, Jagan institute of Management Studies, Sec-5 Rohini, Delhi, India*
[3]*Associate Professor, Information Technology, Jagan institute of Management Studies, Sec-5 Rohini, Delhi, India*

Abstract: ***IoT has radically altered the workings of IT and networking environments, with significant benefits from wireless sensors and nanotechnologies. Although IoT is a growing forum, current data protection and security analysis has demonstrated that security and data security cannot be combined and united and that it will affect the use of the methodology for fear of personal information. Up to now, the polls have focused on vulnerabilities based on Internet-based information exchange technology. None of the polls have identified the user-centered integrated view on privacy and security. The main aim of this paper is to analyze the current state of IoT and to highlight the activities in the area of data security and privacy threats, surface attacks, vulnerabilities, and counteractions, and to suggest a taxonomy of the danger. To demonstrate basic user safety and privacy needs and concerns, IoT user's requirements and challenges have been identified and debated.***

Keywords: Advancements in IoT, Cyber Attack, Data Security, Internet of Things, Privacy Threats

I. INTRODUCTION

Just as we hear the word internet, two things come to our mind: first a lot of data and second security and privacy issues. We all use the internet in our day-to-day life from smart homes to smartphones from smart cities to connected vehicles. The Internet has shown a remarkable shift with the evolving needs of applications. With an increase in the number of internet users, day by day the amount of data is also increasing and since 2011 the data has been almost doubling every two years. Now as data is growing at such a tremendous speed that it is introducing a whole new set of privacy concerns for consumers. Every device a consumer is using nowadays collects personal information and with a lot of data breaches going on it has developed a major concern in the minds of the consumer like am I vulnerable to a cyber attack? or is my personal information safe or not? These questions are suggesting some hints towards future research. This paper will help all of us in examining various types of security attacks for gaining credentials.

The ITU-T 13 research team explains the Internet of Things (IoT) as data that provides advanced services by connecting things (physical and virtual) based on existing and evolving communication and information technologies. The IoT global market is predicted to expand enormously by 28 billion by the end of 2020.

With heterogeneous devices. IoT-objects can create a huge quantity of data that seriously threatens the privacy and security of the individual, as their activities can be tracked everywhere and anytime. The major security threats to consumers are 1. Use of personal information without the consent of the user. 2. Increase in different types of security attacks on various systems that may even include asking for a ransom.

This paper addresses thoroughly the primary constraints of existing works such as accessibility, authentication, data confidentiality, data security, and identification. Consequently, the main goal is to give the reader a complete discussion on the latest IoT technology, with a focus on the actions taken in the areas of privacy and security risks, vulnerabilities, and their available countermeasures.

First, user approval needs to make the information sharing transparent. Secondly, many of the stakeholders who work in the respective system need to adapt the authorization and use management model. Thirdly, each system should use the data anonymization method to be trustworthy for various combinations of different sets of data.

This paper investigates the privacy of the IoT from the viewpoint of users, It addresses broader security standards, and frames the IoT security environment by IoT devices' resource constraints. The paper also covers IoT architecture with the principles of privacy and security. It also highlights open questions and research recommendations in the latest trends of privacy and security in IoT.

The remainder of the document is divided into four sections: Section 2 covers the progress made in the IoT security field, and in the next section, i.e. section 3, the developments in IoT privacy are included. Section 4 tells us how the IoT bugs can be reduced. And this paper will end in section 5.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue V May 2021- Available at www.ijraset.com

II. MAJOR ADVANCEMENTS IN IOT SECURITY

In this section, we will review the advancements done in IoT Security. We know that users face a lot of security challenges, the more the devices are getting connected more the users feel less secured as any one thing gets hacked the users might end up losing all of their secured data. Let us observe a few pieces of literature to explore what's going on in the security field and any advancements that are being done here. How we handle IoT safety determines if it changes the way we live and operate. Although protection was a concern with the standard web, security issues posed new and unusual security problems in the IoT context. The overarching focus should be the addressing of these issues and the safety of IoT goods and services. Users should be assured of the security of IoT devices and related data services, particularly because this technology has become more common and integral in our everyday lives.The biggest task is to integrate protection and user acceptance processes. Instead of assuming the machine controls them, the user should feel he is manipulating all details relevant to them. This incorporation creates new criteria which, as far as we know, have not previously been considered. Safety issues the safety of embedded computers and networks within the framework of IoT. Defense from unauthorised data access, Internet threats, denial of services on dawns, unauthorised services access, data misuse or modification, malicious attempts and network security. IoT encryption ensures protection from unauthorised data access. However, IoT is likely to contribute to the proliferation of malicious attacks through its ability to communicate and control various networked automated devices over the Internet and remotely [2,15].
Abdur et al. [12] focused on trust, access control and data privacy.
Therefore, the following points out the different security issues in the IoT setting as summarised in Table 1.

A. Identification

1) For a smart computer, it is most important to know whether the name can be revealed or not. A significant danger may arise from the identification of an adversary[10].
2) We must, therefore, acquire a scheme that provides other eligible devices with user identification at the same time. Devices interacting with consumers (humans) need to know and discern between their identities[9]

B. Data Integrity

1) A number of other non-compatible causes, such as transfer data shift, the server shutdowns and electromagnetic interference, may be affected by cybercriminals[10].
2) Data integrity is a common tool for monitoring the use of cyber criminals to secure the valuable information and to avoid external intrusion after it has been sent and received.
3) So, without detecting a hazard, the machine cannot adjust the data[1]. Checking and Cyclic Redundancy (CRC) checks are used by error detection systems [10] to guarantee data consistency and durability .

C. Data Confidentiality

1) The data secrecy means that users rely on different methods to avoid unwanted disclosure [1] to protect sensitive information.
2) Data privacy-proof security measures include data encryption that protects data against unauthorised entry, two-stage authentication providing two-dependent part authentication, and biometrical authentication which is detected individually [1,2].
3) This guarantees that sensing networks do not reveal sensor node data to surrounding nodes and send label data to unauthorised readers for IoT-based devices [1,2].

D. Authentication

1) Authentication is difficult because authentication infrastructures and servers are generally required for achieving their goals by exchanging relevant messages with other nodes.
2) Such methods in IoT are not viable as passive RFID tags are unable to share so many messages with authentication servers. The sensing nodes [1,9,10] are also subject to the same argument.

E. Data Privacy

1) Due to the abundance of expanded data volumes in the IoT setting, it is much more serious to understand the current challenges of using data for reasons other than or in addition to those originally defined.
2) The IoT world has cameras, sensors, reading devices and apps that can capture a wide range of different data forms and people through these areas. Due to the summary statistics, it is possible to identify persons.[2,9,12,30]

F. Access Control

1) Access management applies to resource use authorisations allocated to various IoT network actors. Instead of per-device granularity, access monitoring should be focused on IoT capabilities because variables impacting access management decisions are highly context-based.

2) A variety of steps are required to specify and authenticate the necessary smart device access control. [9,16]

Security Concerns\Refrences	[8]	[14]	[9]	[12]	[11]	[10]	[1]
Identification	✔	✔	✔	×	×	✔	×
Data Integrity	✔	×	✔	×	×	✔	✔
Data confidentiality	×	×	✔	×	✔	✔	✔
Authentication	✔	×	✔	×	×	✔	✔
Data Privacy	✔	✔	✔	✔	✔	✔	✔
Access Control	×	×	✔	✔	×	×	×

Table.1 summary of different surveys

References	Threat Level	Threats and security challenges
M. Farooq et al (2015)		• An **Eavesdropping attack**, also called a sniffing attack. • It is a theft of information that is transmitted through a computer, a smartphone or another linked device through a network. • This may end up affecting confidential information.
E. Leloglu (2017)		• A **spoofing** attack occurs if a malicious person impersons a device or user onto a network to attack, rob data, spread malware or circumvent network host controls. • Some kinds of spoofing attacks are possible for malicious parties to perform. • Amongst the most popular approaches are IP address spoofing attacks, ARP spoofing attacks and attacks on the DNS server.
C. Ramakrishna et al 2018		• In **Man-in-the-Middle attack (**MITM) the attacker secretly alters the communication between two parties. • Here victims think that they are communicating directly with each other but the whole conversation is under the control of an attacker
M. Premkuma et al 2019		• **Dos Attacks** are normally performed to render a device unavailable and mostly by flooding traffic in the system. • This means that legal users cannot access the required services
A. Mohaisen 2013		• **Malicious code injection** may change the code into a vulnerable program and if this program gets executed fully then we may end up losing all of our control over the system. • Other problems can also arise like loss of data or data corruption.

E. Leloglu 2017 F hu 2016		• **RF Jamming** works by reducing the signal to noise ratio that can disrupt the communication.
M. Farooq et al 2015		• **Sybil Attack** is a harmful attack when we talk about sensor networks. • Here we have a malicious node that may act as other nodes or this single node may behave as if there are a lot of nodes
A. Mohaisen 2013 J. Gupta et al 2015		• **Sinkhole Attack** prevents the base station from getting correct and complete sensing data. • This way the legitimate data packets are misrouted and attackers can gather sensitive information
A. Mohaisen 2013 J. Gupta et al 2015		• **Spear Phishing Attack** is one of the most successful attacks where the attacker disguises himself as one of the knowns of the victim and then tries to steal personal information by using email or other online platforms.

 High Level Risk  Medium Level Risk  Low Level Risk

Table. 2 THREATS AND SECURITY CONCERNS IN IOT

III. MAJOR ADVANCEMENTS IN IOT PRIVACY

IoT systems store, interpret and communicate network critical data. This data needs sufficient security against opponents, as long as the customer knows what personal data was stored.

The Cavoukian[17] definition of privacy by design is quite generalised and there are no specific implementation techniques in the device design approach. In this article, Hustinx presents the following additional concepts to bridge the void found in the evaluation of the seven guidelines identified by [17].

1) *Data Minimization:* Through consistently minimising the volume of data gathered and stored, preventing privacy hazards. Therefore, unexplained connections and processes should commence by necessity with applications, information and communication technologies and system construction.
2) *Informed Consent:* The words are clearly, appropriately and transparently presented. This encourages users to opt not, even as allowed by statute, to exchange such material. The privacy of the data defines the consistency of the requisite consent.
3) *Transparency:* It gives users a clear overview of how data is processed and then used.
4) *Verifiable Preventive Protection:* By validating security measures we can improve our security and then prevent threats.
5) *Possibility To Withdraw Consent:* Here users can easily remove their common data and can withdraw their consent anytime.

A. Privacy Challenges

Confidentiality has been a significant issue in the growth of IoT and the dissemination of technology. In the Internet of Things the compilation, usage and sharing of user data is popular and continues. The study [18] discusses the most frequent privacy risks to the internet.

1) Identification is a significant hazard that identifies people such as names and addresses. Essentially, we have expertise with the back-end services of the IT model, with vast quantities of information concentrated beyond the reach of the subject in a single position. In IoT, however, interaction and data collection are also important as the threat of identity increases with the impacts of new technology and the existence of encounters and interactions.
2) The location and tracking of people with various tools, such as GPS, Internet traffic, smartphone location, etc. are dangerous. Infringements of privacy, such as recording of GPS, exposure of personal details such as disease or surveillance or regulation pain, have been found.

3) Profiling is used to customise the e-commerce (e.g. news and ads). Organisation, when engaging with other accounts and data points, collected knowledge of importance. Data streams are exploding every day as IoT progresses. Moreover, while the processing of data increases quantitatively, the analysis of the previously inaccessible aspects of a person's personal life differs qualitatively.

4) Interactions and presentation share a range of intelligent objects and creative ways to communicate and provide users with input. This violates anonymity and customer-to-personal knowledge.

5) When IoT goods are sold, used and discarded by their users, the life cycle transformations occur. Objects have been shown to delete all evidence, but intelligent systems also retain vast quantities of past data during their lives. This includes personal photographs and videos not removed during ownership transition.

6) Attacks are used to collect intelligence about illegal use of personal objects and features and to access them. Thieves may use inventory data to find safe time for property identification and destruction

The seven privacy risks are classified as low to moderate threats. Confidentiality is also a major obstacle to IoT once users support it. It remains one of the most severe risks with an elevated privacy score among the challenges. Our analyses show a significantly wider range of risks and that more connected data is added to the risks such as profiling and monitoring, while at the midpoint they cause clear, basic privacy concerns.Note that business models which are strongly dependent on profiling have had considerable success, and therefore a push for big data goes on, driven by the core pledge of IoT to gather sophisticated and omnipresent data. The challenge here is to develop IoT-based privacy technologies to balance business priorities and privacy needs of consumers. Privacy risks like contact and appearance and transactions in the lifecycle are ranked medium because they affect consumer profiling. Attacks on links and inventory have low ratings of hazard.

References	Threat Level	Privacy Threat	Challenges
M. Abomharav et al 2015		Profiling	• Data about consumers may be collected in conjunction with other data points and accounts to determine their preferences. • If unwanted advertisments, price discrimination and social engineering were used for the data, profiling may cause privacy violations. • In creating and reviewing data profiles, the user's preferences must be balanced with the user's privacy criteria. • Collecting and selling customer accounts on the data market without the individual's agreement is also seen as a privacy violation.
K. Rose et al 2015		Identification	• The IoT system design enables centralized communication and horizontal communication. This eliminates the available identity data beyond the personal domain of the user and restricts the attack vector. • The challenge is to associate the identity in a specific environment that breaches the privacy of the individual by giving identifying information to organizations outside the personal domain of a user and increasing the potential vectors of a cyber attack.
K. Rose et al 2015		Localization and tracking	• The danger is linked to the location of the individual across time and space. • While it is currently possible to locate and track data using different methods, such as internet traffic and mobile telephone GPs, many people may interpret it as privacy violations when data are misused, or if the sharing of their location data was not controlled [93]. • The IoT also faces a challenge to ensure that the location data is tracked and controlled.

M. Abdur et al 2017		Privacy-violating interaction and presentation	• Most of the processes employed for interacting with the user and the input information currently available are intrinsically public and pose a privacy threat if other people can observe the data[39]. • The IoT must then solve the problem of convenient visibility of personal user information.
G. Baldini et al 2018		Lifecycle transitions	• During modifications to the control spheres of the gadget during their lifetime, private information obtained by users during IoT devices can be revealed. • The intelligent devices communicate with countless services and people and collect data in their history logs about such interactions. Considering that customers who have the products forever own the life cycle for most consumer goods, the selling or sharing of these products might lead the purchaser to access sensitive data concerning the previous owner and thereby violate the privacy of the person.
H. Lin et al 2016		Inventory attack	• As IoT connectivity capacity develops as a whole vision develops, both legitimate and non-legitimate parties should search the smart devices over the internet. • If non-legitimate organizations request IoT gadgets, they may use the device to gather unauthorized information about the features and the existence of personal effects of the user. • The IoT would therefore allow the communication, posing a threat to their privacy, of extensive data about the lives and properties of the users. • To discourage passive inventory attacks from something clever based on fingerprints is a mechanism that adds tolerance to fingerprints. Inventory attacks will surely be hard to resist. While PET is intended to protect privacy, currently it is not the best but most adequate solution among the masses that can make fingerprints even easier.
N. Aleisa 2017		Linkage	• First, user approval needs to make the information sharing transparent. • Secondly, many of the stakeholders who work in the respective system need to adapt the authorization and use management model. • Thirdly, each system should use the data anonymization method to be trustworthy for various combinations of different sets of data.

 High Level Risk  Medium Level Risk  Low Level Risk

Table. 3 CHALLENGES IN PRIVACY

IV. COUNTER MEASURES

To ensure the privacy and protection of users should start by considering what users are before they start using IoT. Evaluation of designers and engineers, how users think about their protection, their own among other factors Motivation to proactively secure the privacy you trust interconnected devices because these factors

Impact the interactions between consumers and their computers. For example,

The average person does not have enough numbers and the kind of threats connected to the internet that may be the part he or she should play in revealing himself[19] and
securing facts about him or her.This can be improved; an enhanced understanding of privacy breaches and vulnerability is linked to the number of protection measures reported by users[20]. Below are countermeasures like the entry and authentication checks, protection policies, intrusion prevention, single sign-in, confidence-building, security tolerance, design privacy, and safety tools.
In addition to architecture guidelines from other research, Zeng & Roesner [21] applied access control policy[22] to develop a smart home access control scheme. Four forms of access controls were included:

1) *Reactive Access Control:* If a user tries to use a computer that is not allowed to use it, it will seek authorization in realtime from a more privileged user by sending a message requesting their approval or refusal.
2) *Site-Based Access Control:* If users are not physically close to the computer, users will be prohibited from accessing devices.
3) *Supervisory Access Control:* It Allows restricted users to run the computer if and only when another (authorised) user is nearby *otherwise permissions will not be granted*
4) *Access Control:* A task — an administrator, a child or a visitor is allocated for each account. The access management policy can only be modified, new users added and the devices organised by administrators.

[23] Proposed a security protocol to facilitate the sharing of data between objects, and coupled with an embedded systems security architecture to strengthen security, confidence, and privacy.
In order to make the protocol consistent with the constraints of IoT applications, it was proposed to produce lightweight symmetrical encryption and asymmetric encryption in the Trivial File Transfer Protocol (TFTP).
[24] suggested the HlcAuth key-free system of communication to IoT networks. In principle, HlcAuth used challenge–response processes for reciprocal authenticity between gates and intelligent devices without key management. that HlcAuth can defend against replay attacks, message-forgery attacks, and man-in-the-middle attacks. However, for HlcAuth to work, the authors assumed that attackers are not within a certain range (at least 4.2 m) of the gateway node.
The recognition of individual users who are part of the IoT is another significant security measure for the effectiveness and development of the IoT system. You accessed the IoT computers, which were freely accessible via the default login or password. (SCADA devices, web cameras, traffic controls, and printers). The findings revealed that all of these instruments were still available. If users have been unaware of security and have used minimum security, such as the default product password, this may do more damage than good.If one of the devices is able to target the whole network.One feasible approach is design protection, in which consumers have the tools to access their own records. The alternative is not far away from the truth today. Whenever users generate a data fragment, dynamical consent tools can now be used that allow those providers to view as little or as many of these data as they choose.

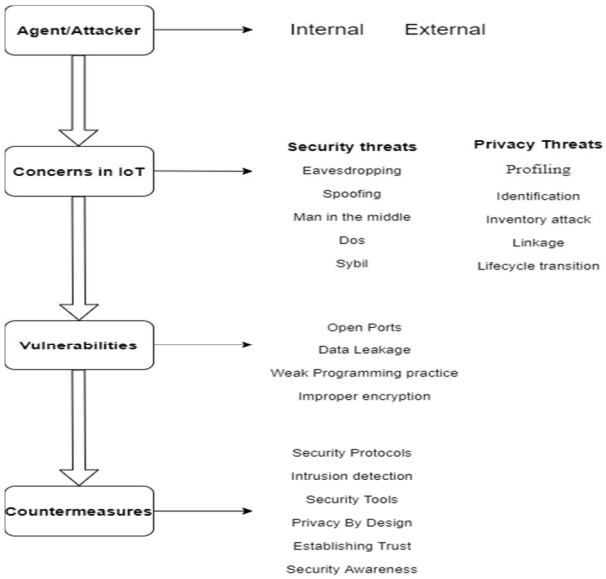


Fig.1 Threat Classification

V. CONCLUSION

The main purpose of this paper is to examine the key features of IoT with particular emphasis on protection and privacy issues. We also examined several other academic articles in this paper to get a basic understanding of where we will be going. This paper helps users to rely on IoT devices so that they can connect and exchange information internationally without being aware of security.

We identified risks and bugs that could prevent users from using IoT technologies in this article. The challenges to IoT security include eavesdropping, spoofing, RF jam timing, assault on Sybil, sinkhole attack and a man in the centre attack and the attack against denial of service. Data protection risks include authentication, positioning and monitoring, targeting, communications and presentations, on the other hand. In addition, this paper outlined some core weaknesses that can allow an attacker to penetrate IoT networks or computers and steal information and other sensitive information from himself. The three major vulnerabilities that devices might reveal include open ports, low passwords, lack of security mechanisms and poor programming. For the improvement of protection on IoT computers, these main considerations should be taken into account: entry and authentication controls, single sign-on, confidence building, security tolerance, and design-based privacy.

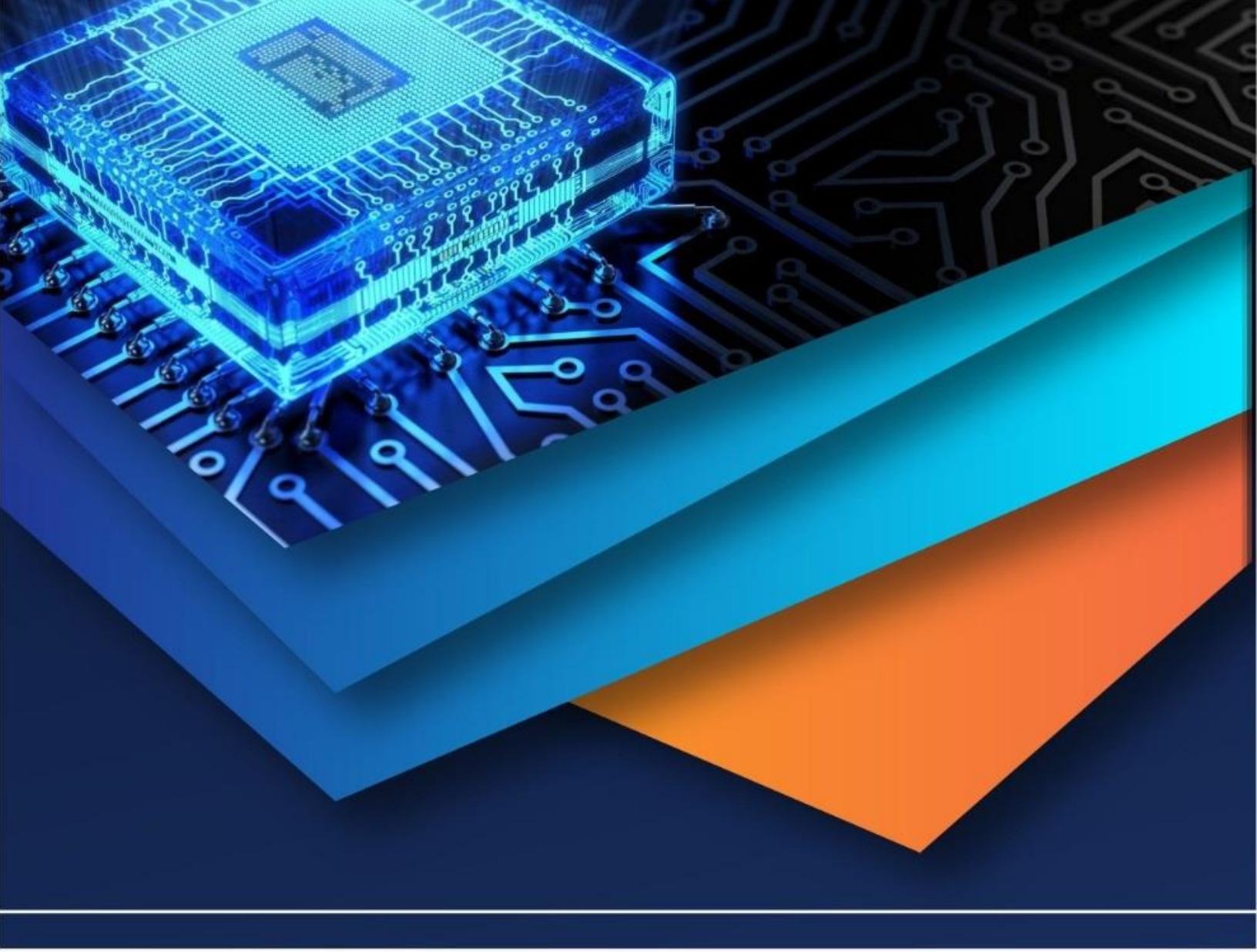
Analysis and classification of IoT safety and data protection aspects are the first contribution of this work. Security risks including malicious code injection and denial of service attacks are large while RF jamming, sybil, sinkhole assault and sniffing are medium-sized. Phishing with spear is considered poor. These risks may reveal IoT systems and devices' weaknesses, which contribute to effective attacks on IoT properties. Regarding the privacy of IoT, profiling is the greatest threat to other challenges such as detection or monitoring, which add to their risks at medium level through the provision of even more linkable information. Threats to confidentiality, such as contact and display, and life cycle transactions, are considered medium because they often influence user profiling. Attacks on links and inventory have low ratings of hazard.

As far as security is concerned, consumers expect devices to secure proactive IOT identifying and protecting against arbitrary assault (for example dos and man-in-the-middle attacks) and misuse at architecture and execution times proactive identifying IOT and defence against malware. In the field of user privacy, this paper established what users want: (a) personal data access (data privacy) and the physical location of the person (personnel privacy), (b) user identity management methodologies and tools. In the field of trust, users wish to share critical, safe and confidential details easily and naturally and to have trust in the architecture of IoT.

REFERENCES

[1] M. Farooq, M. Waseem, A. Khairi, S. Mazhar, A critical analysis on the security concerns of internet of things (IoT), Int. J. Comput. Appl. 111 (7) (2015) 1–6
[2] E. Leloglu, A review of security concerns in internet of things, J. Comput. Commun. 5 (2017) 121–136.
[3] F. Hu, Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations, CRC Press Taylor & Francis Group, 2016.
[4] C. Ramakrishna, G.Kiran. Kumar, A.Mallikarjuna. Reddy, P. Ravi, A survey on various IoT attacks and its countermeasures, Int. J. Eng. Res. Comput. Sci. Eng. 5 (4) (2018) 2320–2394.
[5] M. Premkumar, T.V.P. Sundararajan, K. Vinoth Kumar, Various defense countermeasures against dos attacks in wireless sensor networks, Int. J. Sci. Technol. Res. 8 (10) (2019) 2926–2935.
[6] A. Mohaisen, The sybil attacks and defenses: A survey, Smart Comput. Rev. 3 (6) (2013).
[7] J. Gupta, A. Nayyar, P. Gupta, Security and privacy issues in internet of things (IoT), IJRCS - Int. J. Res. Comput. Sci. 3 (2015) 18–22.
[8] L. Atzori, I. Antonio, M. Giacomo, The Internet of Things: A survey, Comput. Netw. 54 (15) (2010) 2787–2805
[9] A. Riahi Sfar, E. Natalizio, Y. Challal, Z. Chtourou, A roadmap for security challenges in the Internet of Things, Digit. Commun. Netw. 4 (2) (2018) 118–137.
[10] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-porisini, Security, Privacy & Trust in Internet of Things : the road ahead, Comput. Netw. (2015) 146–164.
[11] D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, Ad Hoc Networks Internet of things, : Vision, applications and research challenges, Ad Hoc Netw. 10 (7) (2012) 1497–1516.
[12] M. Abdur, S. Habib, M. Ali, S. Ullah, Security issues in the internet of things (IoT): A comprehensive study, Int. J. Adv. Comput. Sci. Appl. 8 (6) (2017). [39]
[13] R. Uttarkar, P.R. Kulkarni, Internet of things : Architecture and security, Int. J. Comput. Appl. 3 (4) (2014) 12–19.
[14] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (IoT): A vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (2013) 1–19
[15] Wind River Systems, Security in the internet of things, 2015.
[16] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani, Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations, IEEE Commun. Surv. Tutor. 29 (3) (2019) 2702–2733.
[17] R. Roman, J. Zhou, J. Lopez, On the features and challenges, Comput. Netw. 57 (2013)
[18] J.H. Ziegeldorf, O.G. Morchon, K. Wehrle, Privacy in the internet of things : Threats and challenges, Secur. Commun. Netw. (2014) 2728–2742
[19] M. Harbach, S. Fahl, M. Smith, Who's afraid of which bad Wolf? A survey of IT security risk awareness, in: Proc. Comput. Secur. Found. Work., Vol. 2014-January, 2014, pp. 97–110.
[20] R. Kang, L. Dabbish, N. Fruchter, S. Kiesler, My data just goes everywhere:' User mental models of the internet and implications for privacy and security, in: SOUPS 2015 - Proc. 11th Symp. Usable Priv. Secur., 2019, pp. 39–52

[21] E. Zeng, F. Roesner, Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study, in: Proc. 28th USENIX Security. Symp., 2019, pp. 159–176.
[22] W. He, et al., Rethinking access control and authentication for the Home Internet of Things (IoT), in: Proc. 27th USENIX Security. Symp., 2018, pp. 255–272.
[23] M.A.M. Isa, N.N. Mohamed, H. Hashim, S.F.S. Adnan, J. Manan, R. Mahmod, A lightweight and secure tftp protocol for smart environment, in: 2012 IEEE Symposium in Computer Applications and Industrial Electronics, ISCAIE, 2012, pp. 302–306.
[24] C. Li, et al., HlcAuth: Key-free and secure communications via homelimited channel, in: ASIACCS 2018 - Proc. 2018 ACM Asia Conf. Comput. Commun. Secure, 2018, pp. 29–35.
[25] M. Abomhara, G.M. Køien, Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks, J. Cyber Security. Mob. 4 (1) (2015) 65–88.
[26] K. Rose, S. Eldridge, L. Chapin, The Internet of Things : An Overview, No. October, Internet Soc, 2015.
[27] G. Baldini, M. Botterman, R. Neisse, M. Tallacchini, Ethical design in the internet of things, Sci. Eng. Ethics 24 (3) (2018) 905–925.
[28] H. Lin, N. Bergmann, IoT Privacy and security challenges for smart home environments, Information 7 (3) (2016) 44.
[29] N. Aleisa, K. Renaud, Privacy of the Internet of Things: A Systematic Literature Review, in: Proc. 50th Hawaii Int. Conf. Syst. Sci., 2017.
[30] Suman madan, Puneet Goswami;(2020) Adaptive Privacy Preservation Approach for Big Data Publishing in Cloud using k-anonymization, RACSC(Recent patents on CS), vol 14, pp 2689-2690, DOI : 10.2174/2666255813999200630114256



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY