

Challenges in Internet of Things & Security Solutions Approaches

Mrs. Neha S. Patil¹ and Dr. Jaydeep B. Patil²

¹AISSMS IOIT/Computer Science and Engineering, Pune, India

Email: neha.patil@aissmsioit.org

²D.Y. Patil Agriculture and Technical University Talsande/CSE, Kolhapur, India

Email: jaydeeppatil@dyp-atu.org

Abstract—We live in the age of the Information Revolution. Today, ordinary gadgets such as cell phones, TVs, vehicles, etc. are increasingly turning into smart phones, smart TVs, smart cars, etc. And to make it smart, the Internet plays an important part. Basically, the idea of the internet of things is based on the internet, and things mean that things are related to the internet. The idea of smart cities, smart hospital, wireless sensor network, home automation are future of countries all these required IoT. These technologies are IOT-based anywhere, and these technologies need to establish a connectivity route to data transfer that can contribute to several security issues. Using the Internet of Things to connect all the devices and monitor them by the user, risk factors could escalate while sending a lot of information to create a correct connection during computer and user contact. Researcher has worked on IOT also they have faced many challenges to implement IOT. This paper contains the important aspects of IOT with their challenges. So in future researcher can keep these issue in their mind, and it will be very useful to them for further analysis.

Index Terms— IoT, machine learning, privacy, security.

I. INTRODUCTION

While many existing products, such as networked computers or 4G-enabled cell phones, still have a sort of unique identification, the Internet of Things (IoT) contains things that have unique identities that are linked to the Internet. These devices are often connected to the Internet, with the focus on IoT being on configuring, managing and networking devices or 'things' that are not typically connected to the Internet via the Internet. IoT's spectrum is not limited solely to Internet links. IoT can interact and share data with meaningful applications in the direction of a particular user or machine purpose. IoT network applications collect and produce data from lower-level data by filtering, sorting, categorising, condensing and contextualising the details. This collected information is then structured and organised to infer knowledge of the device and/or its users. The world and its practises and progress against its aims, facilitating smarter success.

This paper is organized as follows. Section II explains literature review from different recent papers, Section iii. Explains about IOT features and security requirements, section iv. Elaborates Challenges in IOT, Section v. explain. Internet of things security solutions approaches and final section Conclusion conclude the paper.

II. Literature Review

The authors [5] suggested that several threats, such as jamming and spoofing attacks and other unauthorized access, have undermined the privacy of the knowledge of the user. Potential options are available that can help individuals incorporate different security mechanisms that can help protect their IoT products. Different privacy risks have arisen at present, according to [6], and they may infiltrate IoT technologies and their embedded networks. Managing the security of IoT devices in companies and organizations is not easy. Organization must deploy software for tracking and scanning all IoT devices to identify some form of privacy threats and to reduce the possibility of infringement.

Traffic interceptors and analysers help identify different cyber threats and investigate them. Several research and programs on emerging developments in IoT defense have been conducted [7]. Different services provide threats or vectors for attacks on many IoT devices and their guards. The protocol related to novel IoT protection can be supported by different modelling techniques, models and the availability of several platforms which can support this security protocol. Organization must deploy software for tracking and scanning all IoT devices to identify some form of privacy threats and to reduce the possibility of infringement. Traffic interceptors and analysers help identify different cyber threats and investigate them. Several research and programs on emerging developments in IoT defense have been conducted [7]. Different services provided threats or vectors for attacks on many IoT devices and their guards. The protocol related to novel IoT protection can be supported by different modelling techniques, models and the availability of several platforms which can support this security protocol.

According to [9] the conclusion of a contract consisting of various devices with different communication protocols is one of the most important measures to consider. The discrepancies in protocol are central to the cyber safety system of every internet of things and impede different services contracts from deployment. He showed that some small steps need to be taken to alleviate the complexities of IoT cyber security to ensure that the IoT architecture is reliable in the cybersecurity arena. The writers in [9] have demonstrated that scalability is an integral indicator of the Internet of Things' performance of cyber defense. Analysts suggested that the IoT environment needs to be adequately flexible to solve a billion problems relevant to internet and cyber security.

III. CHALLENGES IN IoT

A. Privacy and Security

Given that IoT has become an important element for the future of the internet by growth in its usage, it needs to address security and confidence functions appropriately. Moreover, on current Wireless Sensor Networks (WSN), IoT has laid the basis of IoT and thus IOT architecturally has the same privacy and protection problems as WSN [3]. Different attacks and vulnerabilities on IoT systems show that a broad spectrum of security principles are required to secure data and systems from end to finish. In general, many attacks exploit deficiencies in some devices to gain access to their networks and thus to vulnerate safe devices [4, 5]. This protection gap also provides inspiration for comprehensive security solutions consisting of successful research into applied data and system security cryptography, non-cryptography security technologies as well as frameworks that help developers build secure systems on heterogeneous devices. More research is required on encryption security services which can run on IoT devices with restricted resources. This will allow various skilled users, regardless of the insufficient user interfaces for almost all IoT devices, to safely use IoT systems and deploy them. In IoT privacy and protection the aspects should cover other areas such as anonymity, trustworthiness, authenticity, integrity of message and additional security requirements.

B. Data Management and Processing Analysis

The encoding, interpretation and data management are extremely difficult because of the heterogeneity of the IoT and because of its large data set, particularly in this era of large data [6]. As a result, most systems rely on current technologies for this problem, such as mobile cloud computing or fog computing, and both on edge processing. The implementation of Information Centric Networking (ICN) in the IoT is another research direction for data management. Since these ICS provide support for the efficient retrieval of information and access to services, they appear very useful not only for access, but also for transfer, manage and transmit content produced. However, it raises many challenges: how to competently expand the ICN model across fixed network lines, how static and mobile IoT devices are to be taken into account and how ICN functions can be allocated on resource-controlled devices [7]. In addition to playing a key role in IoT's development, data interpretation and meaning often pose major problems.

C. Machine to Machine Communication Protocol

While IoT-oriented communication protocols, such as CoAP and Message Queuing Telemetry Transport (MQTT) have already been in place, no open IoT standards are yet applicable. While there is no standard in this area. While all objects require a connection, the Internet cannot be capable of any entity, as it just needs to be able to position its data on a specific gateway. There are also several choices for appropriate wireless technology like Lora, IEEE 802.15.4 and Bluetooth, but the capacity to continue covering the wide range and range of IoT communication is not evident from that moment[2-7].

D. Blockchain

Like IoT, since its launch in 2018, blockchain technologies have also become immensely popular. While Blockchain was used as a crypto-monetary technology underlying the Bitcoin scheme, it is now used for multifaceted, non-monetary applications[8, 9]. Miraz believes that both IoT and Blockchain will improve each other reciprocally by minimising inherent architectural weaknesses [9]. IoT is based on WSN technology. IoT also suffers from protection and privacy concerns analogous to WSN. On the contrary, its built-in protection, immutability, faith, and openness are the key reasons for the blockchain adoption trend in non-monetary applications. These characteristics are driven by the consent and usage of DLTs that involve a heavy dependency on participating nodes.

E. Architecture and heterogeneity

Many researchers have tried to describe different IoT architectural models, some of which are usually applied to a specific field of application. Architecture, especially for a clever office application, was designed by Castellani et al.[13]. This model aims to connect wireless sensor networks and powertrain networks as a web service to the Internet. These facilities, for example door controls, require a trustworthy network and certain recognition technology to give a certified individual the authorisation (e.g., RFID). It has three types of nodes: BSN, MN, and SN (Base station node, Mobile Node, Specialized Node. Based on their versatility, operating range and specialisation, each type has its own attributes. An IPv6 sink or IPv6 router is a static node. It offers direct Internet access.

The three most common components here is M&DC, DCN, which looks like the brain, NoS, which resemble the spinal cord and NoS (networks and sensors). The three main components are nerves. The three main components are M&DC. The Ubiquitous IoT is driven by SOF.

F. Resource management

As IoT is a system composed of many nodes, these nodes are processes and services. These are not just resources. In order to take advantage of the full capacity and gain of IoT, all IoT services should be handles efficiently and effectively .Helsing et al. [14] also approved the fact that software agents would provide for task automation for devices and end-users. They proposed Cougar to support resources management in an IoT system as a scalable and distributed multi-agent architecture. Cougar's key components are the Cougar Component Model (CCM), plugins, Message Transportation Service (MTS), the blackboarding method, persistence, naming, culture, discovery services, servlets and the logical domain model. The CCM is a module for the loading and management of component software components

It is concluded, after reading these documents that many of these plans do not implement storage and thus data protection is not supported, so this may become a problem to be sorted out. Since some of the resource management methods are for a particular application, other IoT application domains cannot be managed. There will then be a change and a common resource management model can be created.

G. Efficient Data Handling

One of its key components is data as far as every paradigm is concerned. The data can be processed, produced, stored and transited data. Data collection is a major obstacle in the case of IoT. Now and then, several researchers speak about the importance of IoT data mining. According to Ma [15], "Data exchange among broad heterogeneous network elements" is one of the most serious issues in the field and the realisation of IoT." To combat uncertainties including lack of uniformity, incoherence, incorrectness and discontinuities, a more intensive interpretation of knowledge is required. Ma [15] also indicated that the process of sharing data on an extensive heterogeneous network is very important.

H. Societal challenges

After addressing the challenges of technology and their integrated literary survey, the present work addresses briefly another challenge, i.e., the challenge of society. As we have already worked out many IoT applications, including several applications for companies in Section 2, the difficulties are unnecessary to tell. Talent infringement is the biggest social problem. In other words, while the world travels with high speed to IoT, the world also lacks the expertise to effectively execute IoT. In order to evaluate the broad data to make an effective use, Mohanty et al.[11] have analysed analysts' problem. Authors proposed to deal with the situation using Big Data and an algorithm-based analysis. The disapproval of the current mass paradigm is another critical social obstacle.

I. Environmental challenges

Technology's success is directly related to the massive challenges involved. With regard to IoT, it is one of the powerful paradigms that promotes the living of the user. IoT has its effect on the physical world, including probably knowledge environments, after the Internet, cloud computing, mobile computing and similar paradigms whose impacts are up to date only. Since the Internet can make it much easier to function in the world of information, IoT makes life much easier for the physical world. Researcher therefore need to focus on low power consumption using IoT. Mihovska and Sarkar [10] suggested that common platforms be used to exchange data on low-power smart devices. They use low-energy solar energy technologies in their IoT platform.

IV. INTERNET OF THINGS SECURITY SOLUTIONS APPROACHES

A. Centralized Approaches

Centralized security approaches are considered ideal for resource-restricted sensor networks, but the common challenge is the scalability of key management systems and the pre-deployable node shared keys. SPINS and the polynomial method are among the traditional unified methods (a centralised architecture for unicast and multi-cast communication in narrow networks consisting of two protection protocols; SNEP and μ TESLA). It is possible to construct a common secret for any pair of knots with polynomial parts [1,3].

B. Protocol-based Extensions and Optimizations Approaches

This is to simplify the protocol, such as compression, without breaking the security features. There are a range of proposed compression schemes, including the compression of IPV6 headers, the extension headers and the regular UDP header in 6LoWPAN (User Datagram Protocol). TLS Session Resumption without Server-Side State, where the server doesn't have a session status, rather than the encrypted server status is offloaded to and from the cache when handshaking, TLS Cached Information Extension allows for the omission of cached information like broad handshake certificate chains.[4]

C. Delegation-based Architectures

Assign computational activities to more efficient machines, such as public key operations in session institutions. A server-based Certificate validation Protocol (SCVP) allows a client to assign a trusted server to the dynamic task of certificate validation or certificate path building. Trust the SCVP server. Another solution to the delegation is Bonetto[2]. It delegates main tasks, such as the gateway, to a more efficient structure. They describe the protocol of the IKE session, in which the GW intercepts the session. After measuring the session key, this key is passed to the restricted system and both pairs can explicitly protect their communication with the session key

D. Hardware based approaches

Additional hardware security modules, such as TPMs, are used to provide a class of security solutions. A Trustworthy Platform Module (TPM) is manipulative hardware that supports cryptographic calculations, especially primitive public-key cryptography. In a secure memory area, TPMs can carry keys such as private RSA keys. The cryptographic accelerator on TPMs can also measure higher performance cryptographic computations. In comparison, with considerably smaller key sizes [1], ECC offers the same degree of protection. ECC is therefore preferred for restricted environments and recommended.

V. CONCLUSION

The goal of this paper is to give the reader a fundamental overview of Internet of Things, The biggest protection and privacy problems due to its exponential expansion, and the forms of rudimentary safety methods and

strategies to protect user data and protected communication. The heterogeneity of the sensors, low-resource and device design of IoT applications means that traditional safety primitives cannot be implemented. Strong network protection infrastructure is needed to prevent unauthorised use of user information, protect privacy and mitigate threats to security and privacy.

REFERENCES

- [1] Hossein Shafagh (2013) "Leveraging Public-keybased Authentication for the Internet of Things" Master Thesis, RWTH Aachen University, Germany
- [2] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, M. Rossi. "Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples". In IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'12), San Francisco, CA (June 2012), pp. 1–7. <http://dx.doi.org/10.1109/WoWMoM.2012.6263790>
- [3] Z. Alansari, N. B. Anuar, A. Kamsin, M. R. Belgaum, J. Alshaer, S. Soomro, and M. H. Miraz, "Internet of Things: Infrastructure, Architecture, Security and Privacy", in 2018 International Conference on Computing, Electronics Communications Engineering (iCCECE), pp. 150–155, Aug 2018, DOI: 10.1109/iCCECOME.2018.8658516.
- [4] J. A. Chaudhry, K. Saleem, P. S. Haskell-Dowland, and M. H. Miraz, "A Survey of Distributed Certificate Authorities in MANETs," *Annals of Emerging Technologies in Computing (AETiC)*, vol. 2, no. 3, pp. 11–18, 2018, DOI: 10.33166/AETiC.2018.03.002.
- [5] A. S. A. Daia, R. A. Ramadan, and M. B. Fayek, "Sensor Networks Attacks Classifications and Mitigation", *Annals of Emerging Technologies in Computing (AETiC)*, vol. 2, no. 4, pp. 28–43, 2018, DOI: 10.33166/AETiC.2018.04.003.
- [6] Z. Alansari, N. B. Anuar, A. Kamsin, S. Soomro, M. R. Belgaum, M. H. Miraz, and J. Alshaer, "Challenges of Internet of Things and Big Data Integration", in *Emerging Technologies in Computing* (M. H. Miraz, P. Ex-cell, A. Ware, S. Soomro, and M. Ali, eds.), (Cham), pp. 47–55, Springer International Publishing, 2018, DOI: 10.1007/978-3-319-95450-9_4.
- [7] J. Cooper and A. James, "Challenges for database management in the internet of things" *IETE Technical Review*, vol.26, no.5, pp.320–329, 2009.
- [8] M. H. Miraz and M. Ali, "Applications of Blockchain Technology beyond Cryptocurrency", *Annals of Emerging Technologies in Computing (AETiC)*, vol. 2, no. 1, pp. 1–6, 2018, DOI: 10.33166/AETiC.2018.01.001.
- [9] Miraz, M.H., "Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies", *Advanced Applications of Blockchain Technology, Studies in Big Data* 60, 2019, DOI: 10.1007/978-981-13-8775-3_7, https://doi.org/10.1007/978-981-13-8775-3_7
- [10] Mihovska, A.; and Sarkar, M. (2018). Smart connectivity for Internet of Things (IoT) applications. *New Advances in the Internet of Things*, 105-118.
- [11] Mohanty, S.; Das, S.K.; Barik, S.; and Rout, M.M. (2016). A survey on bigdata and its challenges related to IoT. *Proceedings of International Interdisciplinary Conference on Engineering Science and Management*. Goa, India, 331-334
- [12] Ning, H.; and Wang, Z. (2011). Future Internet of Things architecture: Likemankind neural system or social organization framework? *IEEE Communications Letter*, 15(4), 461-463.
- [13] Castellani, A.P.; Bui, N.; Casari, P.; Rossi, M.; Shelby, Z.; and Zorzi, M. (2010). Architecture and protocols for the Internet of Things: A case study. *Proceedings of 8th IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM)*. Mainheim, Germany, 678-683.
- [14] Helsinger, A.; Thome, M.; and Wright, T. (2014). Cougaar: A scalable, distributed multi-agent architecture. *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*. The Hague, Netherlands, Volume, 2, 1910-1917.
- [15] Ma, H.-D. (2011). Internet of things: Objectives and scientific challenges. *Journal of Computer Science and Technology*. 26, 919-924.