Sameena Shaik, 2022, 10:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

Security, Threats, and Trust concerns regarding the Internet of Things

Lecturer Sameena Shaik, Lecturer Sangeetha Komandur
Department of Computer Science,
College of Computer Science and Information Technology,
Jazan University,
Jazan, Kingdom of Saudi Arabia.
shaiksam2285@gmail.com , zainabkhan1284@gmail.com

Abstract- Life in the current world has been made easier by an array of devices and equipment which are interlinked to enhance their complimentary performance. Defense, Transport, Healthcare, Energy etc. all use devices that rely on each other and the ability to inter-communicate and complement each other in operations. These are possible through the internet of things that refers to the interconnectivity of interrelated computing devices, digital and mechanical machines with people, objects, and animals via UIDs. IoT enables data transfer over networks without the necessity of the interaction between humans or between humans and computing devices. These capabilities don't exist without risks and threats that related to IoT. Despite the continued growth of IoT and especially with phase 4.0 acting as a catalyst to its growth, there still are vulnerabilities that affect trust on IoT as risks and threats lead to cyber-attacks. Various research has outlined these risks, and some have gone forward to suggest solutions and areas of research in the effort to make IoT more secure. Through reviewing some of these works, this paper seeks to create a more comprehensive perspective of the works alongside a critical look at their strengths and weaknesses in the propositions made; and then suggesting a unified resolution regarding research on the area.

Keywords- IoT, threats, risks.

I. INTRODUCTION

In today's world, we are surrounded by an invisible web, and the web is woven with billions of devices interconnected and leading to smart life with less human interaction and involvement in daily life.

The rapid adaptation of this technology has increased the ratio of objects connected to the Internet than humans. The object can be any device if they can explicitly or implicitly get linked to the Internet. It is used in many areas, like automobiles, smart cities, healthcare, industrial equipment, entertainment, e-commerce, sports, etc. Also, the present industrial phase focuses heavily on the interconnectivity and automation of numerous devices.

However, due to limited resources and high computational complexity of IoT, to large extent IoT frameworks rely on the services of cloud paradigm. Huge volume of data generated by IoT is stored on cloud. Data computation and storage is taken care of by cloud service providers. Furthermore, Li et al [9] pinpoints that besides storage; services like security and protection of privacy are given significant importance. Figure 1 illustrates cloud based IoT architecture.

However, the sensitive data flows from network to network, from application to another across the interconnected systems. The data exposure gives rise to threats and leading the device vulnerable to many attacks. Many security challenges arise due to the vast development of heterogeneous and

interconnected systems. Casola [11] proposes this heterogeneity as important risk factor to physical compromise of devices.

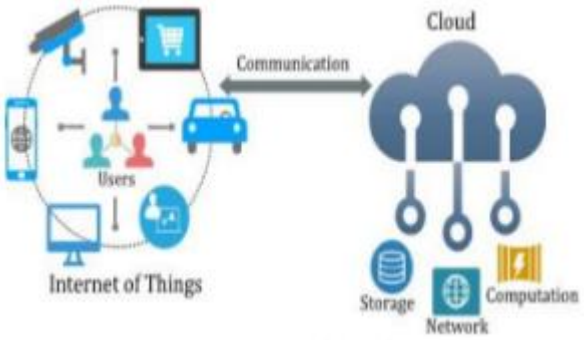

Fig 1. Cloud-based IoT context [9]

The rapidly increasing Internet of Things (IoT) domain, which produces, collates, and exchanges delicate information, gives scope to privacy and security issues in the IoT system. Hence various reviews on IoT privacy and security research have been addressed in this study.

On this review the following aspects are of interest:

- Threats and security concerns of IoT ecosystem and architecture.
- Security and Privacy challenges faced by cloud service providers with respect to IoT context.
- Security features provided by AWS IoT framework.

This is the organization of the paper: After the introduction in section I, section II summarizes the various reviews covered and conducts a comparison of them. The third section elaborates further aspects of IoT and critiques the papers reviewed with respect to security, safety, and privacy concerns that they try to present matters on. Section IV is a brief discussion with a critical lens on the reviewed papers. The section as well offers ideas and proposition of research areas that can further help expound on the papers and make the arguments stronger. Section V is the conclusion of the review.

II. LITERATURE SURVEY

Sicari et al [14] outlines various characteristics of IoT to be able to delve into how those characteristics make IoT vulnerable. The authors point out that IoT is made of up heterogeneous technologies. That implies that those technologies lack uniformity. Each of those technologies has got its own ways through which confidentiality and security is enhanced. Such is done separately from the other devices that are interconnected through the internet of things. Therefore, the traditional security countermeasures such as authentication, use of passwords etc. can't apply directly to IoT technologies owing to the differences in standards and the stacks involved.

This isn't the only problem that they note as far as far as security, privacy, and trust in IoT is concerned. They as well note that the huge number of the interconnected devices brings about issues to do with scalability. As such, to be able to cater for the security and privacy concerns with IoT, a flexible infrastructure is required.

There are three key areas that they identify with regards to the subject matter of security requirements. These include authentication, confidentiality, and access control. Under authentication and confidentiality, their proposal is that there should be a custom encapsulation mechanism specifically intelligent service security application protocol. Confidentiality has several elements that raise queries including confidentiality of outsourced data. For this, which seems the biggest of problems, they propose Discretionary Access control of Mandatory Access Control.

Based on various elements of propositions, indeed **Sicari et al [14]** have done their homework right. Nevertheless, while the solutions presented are great, they still are deficient about addressing the main problem that they point out to be the biggest cause of concern; the heterogeneity of the technologies involved. The solutions are still quite specific and lack an outright one for all solution to the problem of heterogeneity as the biggest concern in developing a cross platform singular solution to security and privacy.

Mahmoud et al [4] do well to help with the understanding of what IoT is which works best to clarify the subject matter to non-computer science related individuals. With IoT being a set of guidelines, protocols, and standards, which simplify implementation of various IoT applications, then anything that complicates these applications would in some way work antagonistically to IoT's very purpose. They note that the success of any IoT application is reliant on the characteristics of the ecosystem of the specific IoT frameworks. Through comparison architecture and security features of

eight frameworks of (AWS) Amazon Web Services, ARM mbed IoT, Azure IoT Suite, Brillo/weave, calvin, HomeKit, Kura and Smart Things, conclusions have been made that indicate a chance for a way forward if security and privacy is to be improved in IoT.

The architecture delves deeper into the one proposed to develop third party applications as well as the compatible hardware and security features.

The authors find that while the same standard is used for securing communications, such as encryption by use of SSL/TLS, different methodologies are used for providing other security properties.

Nevertheless, there are several issues that are problematic as far as standardization is concerned as each framework operates with a certain set of its own rules and guidelines as though each works in an isolated ecosystem. For these frameworks there are differences as far as compatibility is concerned. For instance, while AWS IoT allows IETF class IoT devices to be integrated in its framework, supported by Brillo/Weave. In as far as security is concerned, while each frameworks encapsulates its own security logic, they all do follow the same trend in some aspect in enforcing security standards.

Nevertheless, for both security and architecture features, there still are a few differences. Since the concentration is in security, there is need to consider standardization in other security features besides securing of communication which is the only one that seems to be a bit standardized.

In their paper where the subject matter is the anatomy of threats to IoT, Makhdoom et al [10] agree with Mahmoud et al [4] that the biggest problems facing Io security is lack of standardization and consistency emanating from matters that relate to manageability, operability, and compatibility.

Through looking at various layers and their respective threats, it seems rather obvious that vulnerability isn't just a matter of standardization aspects but also problems to do with due care in the manufacturing of devices. While they do perfect work at analysis of threats and specifically malware threats, there is need for a deeper recommendation on research about the subject matter. Authors of this work for instance take the application layer as an example that can be vulnerability where manufacturers can leave some interfaces in the device hardware open. A recommendation could be a case where due to IoT making all devices interconnected, there is need to revise policies now to stricter measures.

Li, Wang, Lan, Chen, Zhang, and Chen on their part wretle with trustworthiness of cloud. Theirs is more of a proposal of a trust assessment framework. While relevant, it fails to take note that cloud is technically singular and thus trust issues would be usinversa and that a better way of enhancing privacy and security means that practical mechanisms, rather than testing of trust, are necessary.

Moustafa [8] propose Beta Mixture Hidden Markov Mechanism (MHMM) to design threat intelligence. The method is designed to discover anomalies relating to both the physical and network systems. If indeed this can be a solution, then worries of privacy and security would be alleviated. However, despite the suggestion of the methodology, it doesn't address the specifics of problems outlined which mainly are lack of standardization. That means that it is hard to have a one fits all application.

III. THREATS TO IOT

1. IoT Architecture:

Firstly, the IoT ecosystem comprises of IoT hardware and software applications. Hardware refers to sensors, electronic gadgets, servers, hubs and devices that are interconnected on the network either directly or indirect. IoT applications refer to the software that provide functionalities and act as an interface between the connected objects and the users. Figure1 shows a general perspective of interconnection of users, objects, and cloud. For example, a user uses a mobile device to do online shopping through a mobile application.

The online shopping customer's data is stored on the cloud. Sensor devices in a smart-home or smart-vehicle transmit the data over the gateways that are connected on the network. Secondly IoT architecture refers to the complex layout of how these diverse devices are connected to communicate with each other. Due to the vast diverse components and applications of IoT there is no standard architecture for IoT framework.

However, a generalized IoT architecture consists of 4

layers, namely the Physical layer, Network layer, Application layer, and Semantics layer. The physical layer consists of mainly wireless sensors and actuators to perceive information from the environment and convert it for analysis. Based on the routing strategies the scrutinized sensor data gets transmitted over different networks.

The application layer is mainly to assist in data processing, analytic, human-machine interactions, and smart services. Smart services user services like message handling, user authentications and communications take place in Application layer. Aggregated data received from application layer is used by the semantic layer. High end business-related services such as identifying the products, analysis of data, business predictions, decision making are managed by the Semantics layer. All four layers face security challenges.

Table 1. Threats.

Physical Layer	Hardware failure, Unauthorized access tothe device, battery drainage attack, malicious data injection, firmware version, node cloning, device compromise, Sybil attack
Network Layer	Node replication, fragmentation, Dos attacks, spoofing, hello flood, homing, message fabrication/modification/reply attack, network intrusion and device compromise.
Application Layer	Software modification, malicious codes, SQL injection, Cross-site scripting, Identity theft, session token compromise.
Semantic Layer	Identity theft, compromise of user privacy.

Table-1 shows some of the threats that may arise in these layers. In the physical layer data is directly collected by the sensors. The sensors have low computation and storage capabilities. They collect data by perceiving surrounding signals. Sensors are easy target for attackers. Unauthorized alterations to data using malicious injection, hardware failure, access to devices physically, battery drainage, node cloning is some of the security concerns of this layer.

In the IoT framework the data over the network is more insecure compared to the traditional network. The reason is the powerlessness of end devices connected to the network. While the data gets transmitted over the network the attackers can intervene the network and capture the data being transmitted. Moreover, the data can be replicated, redirected to different locations, spooling, reply attack, Dos attack, flooding are some of the concerns that may rise in this layer.

In application layer typically where human- machine interactions take place there is a high possibility of injection attacks like SQL injection and Cross-site scripting. The user's input is deployed with the malicious code to gain access to the users' machine. Identity theft, session token compromise, Brute force are some more examples of attacks that can occur in this layer. Semantic layer is prone to attacks like Identity theft and compromise of user privacy. All the four layers comprising of both hardware and software components of IoT framework are prone to security concerns. Due to diverse IoT Systems with different data context and technologies; standardized protocols are not applied to the ecosystem of IoT that will mitigate the security and privacy concerns to large extend.

The instantaneous revolution and adoption of IoT by industries and business organizations had both pros and cons. Low-cost sensors and end-user devices with low computational capabilities are manufactured. There are problems when it comes to the huge amounts of data that IoT connected devices generate. Also, growth in IoT gave rise to many security and privacy breaches. As a solution IoT relied on the services of cloud paradigms, a third-party service provider. Cloud provides computational and data storage facilities to IoT devices. Hence IoT devices strongly rely on Cloud for their services, therefore, making Cloud an important part of the IoT architecture.

However, the integration of IoT and Cloud not only offers efficient services but also gives rise to several challenges and security concerns. Security and Trust are the two main challenges confronted by the cloud service providers. Currently many cloud service providers (CSP) are available in the market, and many vendors are engaged in developing cloud-based services. Choosing the best one with similar functionalities has become a challenge. Li et al [9]

propose a framework to identify and evaluate trustworthiness of cloud services. A trustworthy CPS should reflect attributes like reliability, availability, scalability, safety, and security. The quality of service and reputation of CSPs determines the choice of cloud services customers preferred by users [9].

A. AWS (Amazon Web Services) IoT Framework In recent years many companies embarked in deploying, troubleshooting, securing, and maintaining IoT applications. Based on the requirements of business IoT frameworks are developed. An IoT framework acts as an interface between the IoT devices and the cloud. Amazon is one of the companies that came up with a cloud platform for IoT named AWS (Amazon Web Services). This paper reviews some of the salient security features provide by AWS IoT framework.

This service leverages a multi-layer architecture for the AWS IoT cloud. To avail services smart devices are securely connected with the cloud and other connected devices. It facilitates the interaction of applications with devices during offline. However, all the smart devices connected to the framework need to be authenticated before the connection is established. Authentication of devices at all points of connection designates the source of data transmission. Also, the data is encrypted before the transmission.

It supports X.509 certificate-based technique for authentication where these certificates confirm the identity and help to identity the public key contained in the certificate. By checking each object, the certificates are verified. Devices connected to AWS IoT are authenticated. The authorization process is policy-based. Device owners write rules in the Rules Engine to authorize devices or applications that can access the device. To and fro communication between devices and applications is encrypted over SSL/TLS protocol. AWS IoT also supports Forward Secrecyn which is secure communication protocol trait. As such, a malicious user who can learn about the private key of an IoT device wouldn't manage to decrypt any communication.

The three main components of the proposed framework include: security-based trust assessment (SeTA), reputation- based trust assessment (RTA), and integrated trust assessment (InTA), are defined. The security metrics used in SeTA were derived from international and industrial security standards (i.e., ISO/IEC, CSA, and FedRAMP) [9].

Fig 2. System model for cloud based IoT [2]

Fig 3. The proposed trust assessment framework for cloud service [9].

It depends on the feedback on the reputation assessment model, and it presented a reputation-based trust assessment method (RTA) to enhance precision and efficiency. The RTA evaluates the reputation of cloud services for fixed- sized consecutive time windows. Local objective reputation: for a specific cloud service in each time window and global objective reputation representing the holistic reputation level of all services provided is obtained.

In addition, a strong combination of SeTA and ReTA is proposed and name as an integrated trust assessment method (InTA) to evaluate the overall trustworthiness of cloud services. The security level and reputation level of a cloud service are provided to the InTA for trust assessment. The proposed methods have been validated through simulation-based experiments; the outcome is efficient and accessible. The limitation is that InTA is not

implemented in a realistic cloud environment. As a future job, the researcher strives to construct a working model for the suggested framework for trust assessment and execute the trust evaluation in a realistic cloud environment.

Makhdoom et al. [10] presented an extensive collection of safety rules which is focused on best industrial procedures that can assist IoT standardization authorities and design to limit the security standards in the IoT apps and devices. The intrinsic security communication protocols do not safeguard the malware and node conceding assaults.

In addition, in the IoT framework, there is an increase in the number of ransom ware attacks, the primary cause of the negative effects could be ascribed to centralized network infrastructure where all network functionality and security activities are efficiently controlled. The limitation is that the infrastructures are expensive to set up, and on the other side, it shows a single point of failure. Thus, in the future, the researcher wants to create a safe Blockchain-based IoT protocol to safeguard the IoT schemes against the attacks on integrity.

Mahmoud et al.[4]presented a comparative analysis of commercially available IoT frameworks and platforms for developing industrial and consumer based IoT applications. The analysis was conducted based on the architecture, hardware compatibility, software requirements, and security. The selected set of IoT platforms include AWT IoT from Amazon, ARM Bed from ARM, Azure IoT Suite from Microsoft, Brillo/Weave from Google, Calvin from Ericsson, HomeKit from Apple, Kuru from Eclipse, and Smart Things from Samsung.

IV. DISCUSSIONS

In the studies addressed, Internet of Things (IoT) security, trust, and threats compared different research-based on the features of the IoT frameworks that concentrate on security, trust, and threats. Authors in [11] address security and privacy issues in IoT at each layer. A study about the cloud service provider, a series of challenging security and trust concerns in the cloud based IoT context. The Authors in [9] proposed a trust assessment framework that can efficiently and effectively assess the trustworthiness of a cloud service.
However, there is still a lot of security gap in the notion of networking devices, and the system is vulnerable to being affected easily. To prevent IoT from vulnerability and threats, it is important to reinforce the IoT devices. Mitigate malicious feedback ratings that affect the trust and reputation of cloud service providers.

V. CONCLUSION

IoT facilitates people's lives in many aspects, but most of the IoT devices are vulnerable to attacks. To build customer trust in IoT, immense importance should be given to strengthen IoT security and mitigate the attacks.

Hence, the research on network security needs to be done to address these issues and provide strong security services to interconnected IoT systems.

REFERENCES

[1] P. K. D. Pramanik, S. Pal, A. Brahmachari, and P. Choudhury, "Processing IoT Data," in Processing IoT Data: From Cloud to Fog—It's Time to Be Down to Earth, 2018, pp. 124–148.

[2] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," J. Inf. Secur. Appl., vol. 38, pp. 8–27, Feb. 2018.

[3] Singh, G. Tripathi, and A. Jara, "A survey of Internet-of-Things: Future vision, architecture, challenges and services," in 2014 IEEE World Forum on Internet of Things (WF-IoT), 2014, pp. 287–292. 10.1109/comst.2018.2874978

[4] M. binti Mohamad Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," Comput. Networks, vol. 148, pp. 283–294, Jan. 2019.

[5] M. Agiwal, A. Roy, and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," IEEE Commun. Surv. Tutorials, vol. 18, no. 3, pp. 1617–1655, Jan. 2016.

[6] R. Boussada, B. Hamdane, M. E. Elhdhili, and L.Saidane, "Privacy-preserving aware data transmission for IoT-based e-health," Comput. Networks, vol. 162, pp. 106–866, Oct. 2019.

[7] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen Porisini, "Security, privacy and trust in Internet of things: The road ahead," Comput. Networks, vol. 76, pp. 146–164, 2015.

[8] N. Moustafa, E. Adi, B. Turnbull, and J. Hu, "A

International Journal of Science, Engineering and Technology

An Open Access Journal

New Threat Intelligence Scheme for Safe guarding Industry 4.0 Systems," IEEE Access, vol. 6, pp. 32910–32924, 2018.

[9] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang, and Chen, "Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach," IEEE Access, vol. 7, pp. 9368–9383, 2019.

[10] Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of Threats to the Internet of Things," IEEE Commun. Surv. Tutorials, vol. 21, no. 2, pp. 1636–1675, 2019.

[11] V. Casola, A. De Benedictis, M. Rak, and U. Villano, "Toward the automation of threat modeling and risk assessment in IoT systems," Internet of Things, vol. 7, pp. 100–56, Sep. 2019.

[12] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: Areview," Internet of Things, pp. 100–81, Jul. 2019.

[13] M. Alshahrani, I. Traore, and I. Woungang, "Anonymous mutual IoT inter device authentication and key agreement scheme based on the ZigBee technique," Internet of Things, vol. 7, pp. 100–61, Sep. 2019.

[14] zSicari, S., Rizzardi, A., Grieco, L., & Coen Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164. doi: 10.1016/j.comnet. 2014.11.008