A Systematic Literature Review on the Security Challenges of Internet of Things and their Classification

Khadija Fazal, Hassan Shehzad, Ayesha Tasneem, Aisha Dawood, Zohaib Ahmed
Department of Software Engineering, National University of Modern Languages (NUML)
Khayaban e Johar, H-9 Islamabad, Pakistan
Khadijafazal98@yahoo.com Hassanshehzad_77@yahoo.com ash_world16@yahoo.com aisha_dawood94@hotmail.com
zhahmed@numl.edu.pk

Abstract—Internet of things (IoT) is an emerging technology. IoT aims at interconnecting devices and people to the internet, but in simultaneously there are some security and privacy threats as security is always critical to software products. The paper focuses on conducting a systematic literature review (SLR) to find out the security challenges in three different aspects of IoT i.e. Devices/Hardware, Networks and Cloud/Server-side, available solutions to address such challenges, limitations to those solutions, existing solutions to address such limitations and the results are then categorized to efficiently and effectively use the existing solutions as well as to pave way for future researches to propose new solutions.

Keywords—Challenges; Cloud/Server-side; Devices/Hardware; Internet of things; Networks; Security.

I. INTRODUCTION

The expression, "Internet of Things" is an arrangement of interconnected gadgets, was initially proposed by Kevin Ashton in 1999 [1]. The Internet of Things (IoT) is a novel outlook change in IT enclosure [2]. IoT is a noteworthy instructive and innovative insurgency. IoT envelopes numerous parts of life from associating homes and urban areas to interfacing autos and streets, streets and gadgets that track an individual's conduct and utilize the information gathered for push administrations [2]. IoT is developing for very nearly 10 years now, where different physical items would be interconnected by the utilization of different existing innovations, such as sensors and Wireless technologies like GSM, UMTS, Wi-Fi, Bluetooth and ZigBee etc. [3]. These physical objects includes refrigerators, televisions, automobiles, household appliances, production machinery, urban infrastructure and cloths etc. that will be uniquely identifiable and ubiquitously connected to each other, collecting some useful information through various existing technologies on the premise of which mechanized moves will be made [4]. Basically Internet of things is about harmonizing the way humans and machines connect using common public services [5].

Gigantic expansion in clients of Internet and progressions in the web innovations empowered systems administration of regular items [6]. "Web of Things (IoT)" is about physical things speaking with each other, machine-to-machine correspondences and individual to-PC interchanges will be stretched out to "things" [7, 8]. People for the most part inside their homes associate with the earth settings like light, air, and so forth, and manage likewise. In the event that the settings of the earth can be made to react to human conduct consequently, then there are a few points of interest [9, 10].

II. BACKGROUND

We have arrived at a critical stage in the evolution of the Internet. Six years back, interestingly, the quantity of "things" associated with the Internet surpassed the quantity of individuals [4]. By 2020, specialists conjecture that 20-50 billion gadgets will be associated with the Internet. Since the gadgets directly affect the lives of clients, the security of the framework must be of high need and there must be some appropriate very much characterized security base with new frameworks and conventions that can restrain the conceivable dangers identified with versatility, accessibility and security of IoT [2, 4]. IoT has an extraordinary potential for adaptability and guarantees an awesome future ahead, however it can cause disaster too, the disaster is in terms of security, as if security is violated nothing remains there [11]. The security may be compromised when we are having millions or trillions nodes connected [11]. Regardless of what amount secure organizations think their items are, they are still required to guarantee appropriate security when any disaster or imperfection is recognized in the framework [3, 11].

The advancement of IoT depends on innovations in numerous fields [12]. Firstly, it is Radio frequency identification (RFID), a remote programmed recognizable proof innovation [12]. It is the center innovation of IoT which is utilized to consequently perceive, distinguish and confirm the remote protests and individuals, through a radio recurrence channel utilizing gadgets called RFID peruses and RFID labels [13, 14]. Also, it is sensor innovation that ought to have the capacity to gather the information from the earth, produce data and caution when the state changes [12, 14]. Thirdly, it is inserted knowledge innovation, which can empower certain essential hubs in a system to process data and reinforce system [12, 14]. In conclusion, it is scaling down innovation and Nano innovation, these...
advancements can add littler items to IoT in order to convey [12, 14].

A. Generic Architecture

Generally, IoT has four key levels as shown below in Fig. 1 [15].

![Generic Architecture of IoT](image)

Fig. 1: Generic Architecture of IoT

1. Perception Layer

The Perceptual layer is the most basic layer also known as recognition layer, collecting information and identifying the physical world through various types of information sensors like RFID, Barcodes, Wi-Fi, ZigBee or whatever other sensor system [16].

2. Network Layer

The network layer is also known as wireless sensor networks, which are responsible for the transmission of information, initial processing of information, classification and polymerization through existing correspondence systems like Internet, Mobile Network or whatever other dependable system [17, 18].

3. Middle-ware Layer

The middle-ware layer comprises of data preparing frameworks that takes mechanized activities taking into account the aftereffects of handled information and connections the framework with the database which gives stockpiling capacities to the gathered information [19]. This layer is administration situated which guarantees same administration sort between the associated gadgets i.e. it is utilized to impart the applications or administrations of the framework, as VMware [19].

4. Application Layer

The application layer provides services for all industries and different handy uses of IoT taking into account the requirements of clients, for example, Smart Home, Smart Environment, Smart Transportation and Smart Hospital and so on [20].

III. RELATED WORK

The arrangement chose for security in implanted gadgets is dependably an issue of exchange off between security, adaptability, execution, power utilization and expense [5].

Existing Solutions to these issues are separated into three methodologies:

- **Software Approach**
  This methodology makes utilization of programmability of implanted General Purpose Processors (GPP) for performing security operations. This methodology achieves the interest in expense and adaptability yet not in the force utilization and silicon zone perspectives [21]. This methodology now and again prompts overpower the handling limit of the inserted GPP [21]. In the perspective of countermeasures against security assault, this methodology can give a few arrangements [21].

- **Hardware Approach**
  This methodology makes utilization of ASICs (Application Specific Integrated Circuits) to actualize a given cryptography calculation in equipment [22]. This arrangement permit controlling exactly the parameters vitality, calculation limit and time requirements yet it is for the most part not ideal for the adaptability and cost parameters [22].

- **Hybrid Approach**
  This methodology is a blend of the two past methodologies [23, 24]. It enhances the general apportioning of usefulness amongst Hardware and Software, and in addition between the framework host processor and security processor, to amplify general preparing productivity while fulfilling other configuration limitations [23, 24]. In Europe, in regards to security perspectives, some underlying work has as of now been performed in admiration of making a characteristic rundown of proper mechanical assurance measures [25, 26].

A universal level, in October 2014, at the International Conference of Data, Protection and Privacy Commissioners in Mauritius, agents of the private segment and the educated community joined together to examine the progressions or dangers that the IoT and Big Data may convey to day by day life. [26, 27]. The administration of gadgets, applications and conventions can be likewise tended to utilizing the standards of administration arranged processing, accomplishing a huge adaptability in various levels of IoT design [28]. To secure remote LAN correspondence, IEEE 802.11 at first gave validation administrations through shared mystery key [29].

A variety of different European projects have started to tackle the research challenges in various aspects of the IoT [30]. Some of these efforts address architectures for efficient integration of the IoT into the Future Internet and corresponding open protocol solutions, others target key enabling services [31], or explore the support of M2M interactions in the communication service layer of future networks, technologies for service layer integration and services and applications [32]. Progress in Internet security protocols provides promising solutions for confidential communications and authentication of the participants with strong cryptographic identities [33].

IoT research works over the developing development of a few related advancements, for example, RFID, WSN gadgets et cetera [34]. Remote Sensor Networks (WSNs)
comprise of little hubs with detecting, calculation, and remote correspondence capacities [35]. Vitality sparing is an imperative test for a WSN [36]. This test turns out to be more basic in huge scale WSNs which convey much greater load and exhaust vitality rapidly [37, 38]. So as to change WSN into a feasible innovation and to make the IoT practical and deployable, there is a need of center product layer arrangements that are completely appropriate with satisfactory guidelines [39, 40]. IoT administrations and applications are as of now turning into a fundamental piece of our general public in our regular life [41]. IoT research works over the developing development of a few related advancements, for example, RFID, WSN gadgets et cetera [42, 43]. A few effective mechanical and scholastic exploration activities are accessible tending to various application areas [44, 45].

A. Security Challenges in IoT

Security is always critical to software products. Classic security challenges in IoT are in three different aspects i.e. Devices/ Hardware, Network and Cloud/ Server-Side, details are mentioned in Table 1 along with security characteristics, in which Cells are represented by letters and an ‘Alphabetic Key’ is assigned to each letter [46, 47, 48].

Table 1: Classic Security Challenges in IoT

<table>
<thead>
<tr>
<th>Security Characteristics</th>
<th>Device/ Hardware</th>
<th>Network</th>
<th>Cloud/ Server-Side</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>A. Attacks on Hardware</td>
<td>B. Encryption with low capability devices</td>
<td>C. Privacy concerns</td>
</tr>
<tr>
<td>Integrity</td>
<td>D. Lack of verification, illegal updates</td>
<td>E. Signatures with low capability devices</td>
<td>F. Unchanged</td>
</tr>
<tr>
<td>Availability</td>
<td>G. Physical attack, radio jamming</td>
<td>H. Unreliable networks</td>
<td>I. Unchanged</td>
</tr>
<tr>
<td>Authentication</td>
<td>J. Lack of user input; retrieval of hardware keys</td>
<td>K. Challenges of using associate identity</td>
<td>L. Lack of widely implemented standards around device identity</td>
</tr>
<tr>
<td>Access Control</td>
<td>M. Physical access; lack of local authentication</td>
<td>N. Lightweight protocols for access control</td>
<td>O. Requirement for user managed access controls</td>
</tr>
<tr>
<td>Non-Repudiation</td>
<td>P. No secure local storage; low capability devices</td>
<td>Q. Signatures with low capability devices</td>
<td>R. Unchanged</td>
</tr>
</tbody>
</table>

A. Security Goals of IoT

Significant security objectives of IoT are to guarantee appropriate identity and authentication mechanisms and to provide confidentiality about the data [49]. The CIA triad is a model used to discuss the security aspects of IT systems, and the same can be extended to IoT, it consists of following three areas i.e. Confidentiality, Integrity and Availability [50, 51]. A breach in any of these regions could bring about serious issues to the system so it is necessary to ensure proper security [50, 51].

IV. RESEARCH METHODOLOGY

The research questions for this study are mentioned in the Table 2.

Table 2: Research Questions

<table>
<thead>
<tr>
<th>SR. NO</th>
<th>RESEARCH QUESTIONS</th>
<th>EXPLANATION OF RESEARCH QUESTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>RQ1</td>
<td>What are the security related challenges in the context of IoT in the peer-reviewed literature?</td>
<td>This research question aims to find out the available security related challenges categorizations in the literature review. The findings of this research question are intended to be used in making a new categorization of security challenges available in the literature.</td>
</tr>
<tr>
<td>RQ2</td>
<td>What solutions are available in the literature to address these challenges?</td>
<td>This question aims to find out the available solutions to address the security challenges found in RQ1.</td>
</tr>
<tr>
<td>RQ3</td>
<td>What changes are required in the existing solutions to improve their usability and usefulness?</td>
<td>The objective of this research question is to find out the limitations of existing solutions and ways of improving them. The identified challenges may result in the development of a new framework, method or a set of guidelines depending upon the results and analysis of RQ1 and RQ2 solutions.</td>
</tr>
</tbody>
</table>

A Systematic Literature Review (SLR) was conducted [52, 53, 54, 55] to meet the needs of the research questions. The research paper work flow is shown below in Fig. 2.

The Fig. 2, illustrates that literature have been reviewed by the researchers of this paper to identify the security challenges in the context of IoT. After their identification researchers categorized the available security challenges on the basis of three aspects of IoT i.e. Devices/Hardware, Networks and Cloud/Server-side. After categorization, available solution for the security challenges were identified from the literature. These solutions may have some limitations, the limitations were addressed through proposed solutions and defining the types of systems to know that which proposed solution would be feasible for which type of system under which condition. The results of SLR were carefully examined and further research was done along with directed brainstorming to address the limitations of existing solutions so as to propose new solution.
V. RESULTS

This chapter holds the aftereffects of systematic literature review using grounded hypothesis system [56, 57, 58, 59, 60].

A. Systematic Review

The results of systematic literature review are summarized in table 3. The results obtained from literature review comprises of challenges, available solutions, limitations, limitations on existing solutions/systems and types of systems are mentioned in section B of chapter V.

Table 3: Resource Based Results of SLR

<table>
<thead>
<tr>
<th>Serial#</th>
<th>Database</th>
<th>Phase1</th>
<th>Phase2</th>
<th>Phase3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IEEE Xplore</td>
<td>736</td>
<td>68</td>
<td>16</td>
</tr>
<tr>
<td>2</td>
<td>ACM Digital Library</td>
<td>6,068</td>
<td>24</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>Google Scholar</td>
<td>24,000</td>
<td>40</td>
<td>15</td>
</tr>
<tr>
<td>Total</td>
<td>3</td>
<td>30,804</td>
<td>132</td>
<td>38</td>
</tr>
</tbody>
</table>

B. List of Security Challenges, Available Solutions, Limitations on Existing solutions, Solutions to Limitations and Types of Systems

Challenges having same solutions have been categorized accordingly along with their limitations, solutions to address limitations and types of systems for which challenges can occur.

C1: Unauthorized Interference between communicating parties [61], C2: Eavesdropping attack [61,63], C3: Trust management [70], C4: NVMs (non-volatile memories) susceptible to physical attacks [63,80], C5: Data Confidentiality, Data Integrity & Data Availability [63,64,65], C6: Device-to-Device identification (Information Privacy) [61,65,66], C7: Access Control[66,11], C8: Insurance of security and privacy requirements in heterogeneous environment [94]. Solutions to address above mentioned challenges are: S1: We need continuous authentication to solve this problem [61]. A secure transmission channel needs to be established between both the communicating entities in a pre-determined time-frame [61 [70]. In short we need: Symmetric/ asymmetric cryptographic algorithms, Hashing functions and Security protocols at network/ transport/ application layers. [61, 66, 65, and 70]

Limitations on above mentioned solutions: L1: Even if the cryptographic algorithms are suitable to be implemented on resource constrained embedded devices, critical aspect is the key management and storage [61, 62]. L2: The IoT administration figures out who can see the information [65]. Solutions to above mentioned limitations: SL1: Silicon physically unalienable function (PUF) has been emerging as a secure object which is able to securely store some cryptography keys, to generate keys and to authenticate device [62, 65]. SL2: It is important to monitor the information from facades. SL3: The system must be able to take proper privacy measures, to do key management and storage and to prevent any unauthorized access. Types of systems: The solutions defined for the challenges will only be feasible if the system is able to take proper privacy measures, to do key management and storage and to prevent any unauthorized access. [61, 63, and 65].

C9: Device Authorization/ Trustworthiness (Redirection of information to wrong receivers) [62, 67, and 49], C10: Security, Quality of Service Management (QoS) and Network Configuration of Wireless Sensor Networks (WSNs) [68], C11: Naming and Identity Management [63]. Solutions to address above mentioned challenges: S2: Applying the IP to the Field worldview, which infers relegating extra obligations to the sensor hubs as a satisfactory answer for coordinate WSNs with the Internet [67, 49].

Limitations on above mentioned solutions: L3: Arrangements are not appropriate for the restricted sensor hub assets and therefore, novel instruments must be created to adjust to the capacities and requirements of WSNs [49, 67, and 68]. Every item or sensor needs an extraordinary personality over the Internet [63].

Solutions to above mentioned limitations: SL4: Examine existing methodologies and find reasonable adjustments for asset compelled sensor stages to handle these difficulties [49, 68]. SL5: Proficient naming and personality administration framework is required that can powerfully allocate and oversee exceptional character for such an extensive number of articles [63].

Types of systems: The solution defined for the challenges are not feasible for the restricted sensor hub assets. In this way a novel instrument should be produced to adjust to the abilities and imperatives of WSNs. Every item/sensor needs an interesting character over the Internet [49, 63, and 67].

Solutions to address above mentioned challenges are: S3: One method is to grow less overhead information encryption strategy for securing information transmission and other is to construct secure trust model to store information in cloud environment [69]. There must be a backup available of the important data at multiple places [69]. In short we need: [73, 81, and 93].

Types of systems: The solution defined for the challenges will be of no use without effective cryptographic mechanism. The transmission framework ought to have the capacity to handle information from vast number of sensor gadgets without bringing on any information misfortune, guarantee appropriate efforts to establish safety for the transmitted information [81, 93].

C16: Heterogeneity and mobility [74, 75, And 94]. C17: Use of standard internet security protocols [64, 81, 85, and 94]. C18: Automated key management [80, 81].

Solutions to address above mentioned challenges are: S4: Secure and Efficient Code Dissemination Protocol for IoT is needed. New cryptographic suite for the security protocols needs to be defined [66]. Limitations are: L4: Credentialing/ registration of devices [94]. Limitations can be addressed through: SL6: Use proper Access control mechanisms and it is necessary to be aware of the troubles, before you interconnect your device [75]. Pairing protocols needs to be followed [94].

Types of systems: The solution defined for the challenges will be of no use if system/ network is non-homogenous/ heterogeneous, compatibility issue may arise.

C19: There are certain challenges related to blocking such as: [87, 91] jamming, malware, C20: Denial of service attack [66].

Solutions to address above mentioned challenges are: S5: Firewall and anti-virus software and Hardware Trojan detection can be used to overcome this challenge. There are no limitations found.

Types of systems: The solution defined for the challenges will be of no use if the system is not available and it does not contain Firewall and anti-virus software and Hardware Trojan detection [66, 87, and 91].


Solutions to address above mentioned challenges are: S6: More open way to deal with RFID is required, which considers different elements outside the store network to collaborate with tokens in an impromptu and important way [89].

Limitations on above mentioned solutions: L5: Standardization, User Interface Provision and Storage Capacity [78, 89].

Types of systems: The solution defined for the challenges will be of no use without Standardization, User Interface Provision and Storage Capacity. Complexity of security and limited resources of RFID tags [78, 89].

C23: Interoperability and Standardization [74, 78, 19], C24: Devices manufactured by various vendors [71].

Solutions to address above mentioned challenges are: S7: The institutionalization of IoT is imperative to give better interoperability to all articles and sensor gadgets [74, 78].

Limitations on above mentioned solutions: L6: Numerous producers give gadgets utilizing their own particular innovations and administrations that may not be available by others [71].

Types of systems: The solution defined for the challenges will be of no use if numerous producers give gadgets utilizing their own advances, administrations and benchmarks which may not be open by others [71, 74].

C25: Secure routing [88].

Solutions to address above mentioned challenges are: S7: Multipath routing and on-demand routing protocols can be applied in the heterogeneous sensing networks [88].

Types of systems: The solution defined for the challenges will be of no use without multipath routing and secure data transmission [88].

C26: Sensing/ Actuation [49, 93].

Solutions to address above mentioned challenges are: S8: This issue can be tended to at equipment level utilizing sensor PUFs [49, 93].

Limitations on above mentioned solutions: L7: They have been generally expected as specially appointed frameworks, with restricted physical expansion and intended to do ordinarily a solitary undertaking [93].

Types of systems: The solution defined for this challenge will be useless if the system does not use sensor PUFs and secondly sensors and actuators are intended to do commonly a solitary assignment [49, 93].

C27: Vulnerabilities in VM-Ware [80, 81].

Solutions to address above mentioned challenges are: S9: The threat can be monitored through Instruction Detection System (IDS) and by implementing firewall [80, 81].

Limitations on above mentioned solutions: L8: May bring about physical harm to them or may change their operation [81].

Types of systems: The solution defined will be of no use if the system does not contain Firewall and detection algorithm [80, 81].

C28: Technological challenges [71].

Solutions to address above mentioned challenges are: S11: The devices/ technologies needs to be upgraded due to technological revolution [71].

Limitations on above mentioned solutions: L9: Zero-Entropy systems, scalability, security and privacy, Communication mechanisms, Integration of smart components into non-standard substrates [71].

Types of systems: The solution defined for this challenge will be of no use if the technology is not upgraded with time [71].
VI. CONCEPTUAL FRAMEWORK

This chapter introduces the proposed structure in subtle element. The proposed system comprises of solid arrangement of characterized ventures as appeared in Fig. 4. These strides are expected to help clients to comprehend security challenges for a given framework. The system is supplemented with security challenges classification given in section B of chapter V. This section B describes the security challenges, available solutions and limitations on the existing solutions/systems, solutions to such limitations and it also describes that in which environment these solutions are best fit.

Security must be implemented in a system while developing it. The developers or manufacturers implement the security in a system during its development. The primary task of the developer is to make the system secure from various challenges. The developer will consult the section B to understand the challenges and to make the system secure from all the challenges defined in this section, through the available solutions defined in the same section to address these issues. There may be some limitations on the available solutions, so the developer will use the proposed solutions to address the limitations. The developer have to check the type of system from the same section to find the best fit for the system being developed.

VII. CONCLUSION & DISCUSSION

Security is always and will be a critical aspect to the IoT network. Thus, it is very important to identify the security challenges in the context of IoT to make it secure from any security breach or violation. In this paper the researchers have conducted a systematic literature review (SLR). By following SLR methodology, three search resources have been reviewed for data extraction to identify the security challenges in three different aspects of IoT i.e. Devices/Hardware, Networks and Cloud/server-side. As if security is violated the IoT network will be destroyed.

The paper defines categorization of security challenges on the basis of three aspects of IoT. The only paper which discusses the security challenges in all aspects of IoT and thus it will be very useful for the researchers to know about multiple security challenges by considering this paper. Types of systems for each challenge is also defined in the paper to understand their system’s behavior and to choose an optimal one for their issues. The paper tries to underline the need of a decent security execution in a stage so clients would be completely fulfilled by their experience and guaranteed that every one of the information is traded while conveying between gadgets.

VIII. FUTURE WORK

In future, researchers can use the work done in this paper to analyze and verify the proposed solutions. The framework defined in the paper, if gets automated, would be really worthy. The researches can also expand their research by including more search resources or databases for data extraction.

REFERENCES


Young Kim, J. Secure and Efficient Management Architecture for the Internet of Things.


