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 meanwhile 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 envelops 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 loT 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 loT 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 loT in order to convey [12, 14].

A. Generic Architecture

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

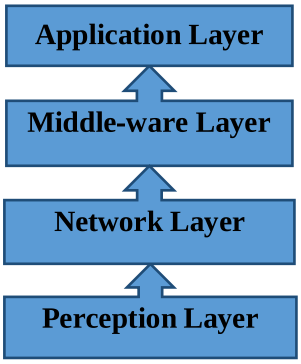


Fig. 1: *Generic Architecture of IoT*

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

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

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

SR. NO	RESEARCH QUESTIONS	EXPLANATION OF RESEARCH QUESTIONS
RQ1	What are the security related challenges in the context of IoT in the peer-reviewed literature?	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.
RQ2	What solutions are available in the literature to address these challenges?	This question aims to find out the available solutions to address the security challenges found in RQ1.
RQ3	What changes are required in the existing solutions to improve their usability and usefulness?	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.

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.

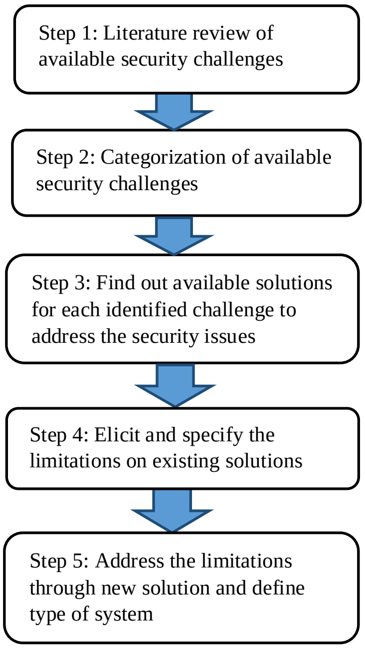

Step 1: Literature review of available security challenges
Step 2: Categorization of available security challenges
Step 3: Find out available solutions for each identified challenge to address the security issues
Step 4: Elicit and specify the limitations on existing solutions
Step 5: Address the limitations through new solution and define type of system

Fig. 2: *Research Paper Work Flow: Step by Step Process*

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

Serial#	Database	Phase1	Phase2	Phase3
1	IEEE Xplore	**736**	**68**	**16**
2	ACM Digital Library	**6,068**	**24**	**7**
3	Google Scholar	**24,000**	**40**	**15**
Total	**3**	**30,804**	**132**	**38**

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].

C12: Transmission and storage of critical data [69], **C13:** Skimming, Tampering, Traffic analysis **C14**: Network security [81, 93], **C15**: Security, Privacy and Legal Accountability [71, 72, and 73].

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].

C21: RFID Security Standards. [89]. **C22**: Interoperability, Scalability, and Abstraction provision, Spontaneous Interaction, Unfixed Infrastructure, Multiplicity, Security and Privacy/ [78]

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].

Solutions to above mentioned limitations: **SL7:** The institutionalization of IoT is vital to give better interoperability to all articles and sensor gadgets [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].

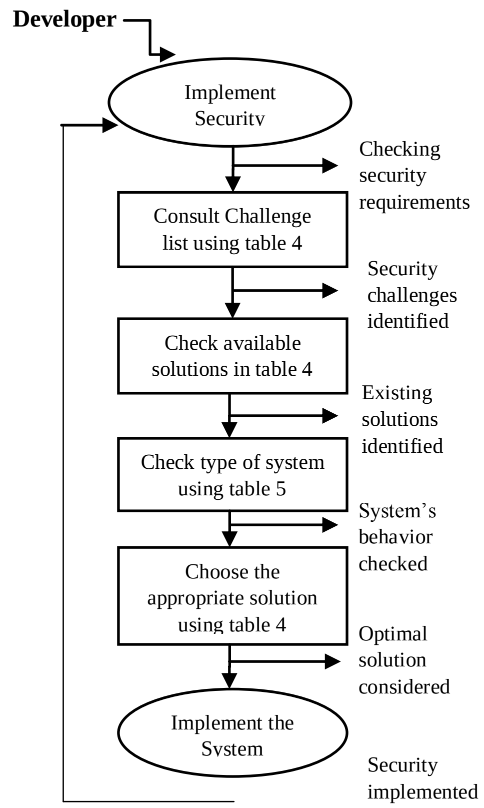
C29: Conflict/ Collision (Multiple RFID tags may transmit data to the reader simultaneously) [70].

Solutions to address above mentioned challenges are: **S12:** Using anti-collision technique can prevent multiple tags from transmitting data to the reader simultaneously and to prevent the reader from reading the data incorrectly (e.g. anti-collision algorithms) [70].

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.


Developer
Implement Security
Checking security requirements
Consult Challenge list using table 4
Security challenges identified
Check available solutions in table 4
Existing solutions identified
Check type of system using table 5
System's behavior checked
Choose the appropriate solution using table 4
Optimal solution considered
Implement the System
Security implemented

Limitations on above mentioned solutions: **L10:** Increases the complexity and cost [70].

Solutions to above mentioned limitations: **SL8:** This requires an additional central control area to calculate the working scope [70].

Fig. 4: *Proposed Framework*

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

[1] Gan, G., Lu, Z., & Jiang, J. (2011, August). Internet of things security analysis. In *Internet Technology and Applications (iTAP), 2011 International Conference on* (pp. 1-4). IEEE.

[2] Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications*, *3*(05), 164.

[3] Mattern, F., & Floerkemeier, C. (2010). From the Internet of Computers to the Internet of Things. In *From active data management to event-based systems and more* (pp. 242-259). Springer Berlin Heidelberg.

[4] Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications*, *111*(7).

[5] Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications*, *111*(7).

[6] Surie, D., Laguionie, O., & Pederson, T. (2008, December). Wireless sensor networking of everyday objects in a smart home environment.

In *Intelligent Sensors, Sensor Networks and Information Processing, 2008. ISSNIP 2008. International Conference on* (pp. 189-194). IEEE.

[7] Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realising the Internet of Things. *Cluster of European Research Projects on the Internet of Things, European Commision*.

[8] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.

[9] Kelly, S. D. T., Suryadevara, N. K., & Mukhopadhyay, S. C. (2013). Towards the implementation of IoT for environmental condition monitoring in homes. *IEEE Sensors Journal*, *13*(10), 3846-3853.

[10] Eisenhauer, M., Rosengren, P., & Antolin, P. (2009, June). A development platform for integrating wireless devices and sensors into ambient intelligence systems. In *2009 6th IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops*.

[11] Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23-30.

[12] Feng, H., & Fu, W. (2010, October). Study of recent development about privacy and security of the internet of things. In *Web Information Systems and Mining (WISM), 2010 International Conference on* (Vol. 2, pp. 91-95). IEEE.

[13] Wang, K., Bao, J., Wu, M., & Lu, W. (2010, October). Research on security management for Internet of things. In *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*.

[14] Oleshchuk, V. (2009). Internet of things and privacy preserving technologies. In *2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace&Electronic Systems Technology*.

[15] Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on* (Vol. 3, pp. 648-651). IEEE.

[16] Zhang, Y. (2011, September). Technology Framework of the Internet of Things and its Application. In *2011 International Conference on Electrical and Control Engineering*.

[17] Gan, G., Lu, Z., & Jiang, J. (2011, August). Internet of things security analysis. In *Internet Technology and Applications (iTAP), 2011 International Conference on* (pp. 1-4). IEEE.

[18] Yang, X., Li, Z., Geng, Z., & Zhang, H. (2012). A multi-layer security model for internet of things. In *Internet of Things* (pp. 388-393). Springer Berlin Heidelberg.

[19] Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December). Future internet: the internet of things architecture, possible applications and key challenges. In *Frontiers of Information Technology (FIT), 2012 10th International Conference on* (pp. 257-260). IEEE.

[20] Jain, A., Sharma, B., & Gupta, P. INTERNET OF THINGS: ARCHITECTURE, SECURITY GOALS, AND CHALLENGES-A SURVEY.

[21] Gebotys, C. H., Tiu, C. C., & Chen, X. (2005, April). A countermeasure for EM attack of a wireless PDA. In *International Conference on Information Technology: Coding and Computing (ITCC'05)-Volume II* (Vol. 1, pp. 544-549). IEEE.

[22] Tiri, K., & Verbauwhede, I. (2005, March). Design method for constant power consumption of differential logic circuits. In *Design, Automation and Test in Europe* (pp. 628-633). IEEE.

[23] Kerins, T., Popovici, E. M., & Marnane, W. P. (2005). An FPGA implementation of a flexible secure elliptic curve cryptography processor. *Applied Reconfigurable Computing-ARC*, 22-30.

[24] Murphy, G., Keeshan, A., Agarwal, R., & Popovici, E. (2006, June). Hardware-software implementation of public-key cryptography for wireless sensor networks. In *Irish Signals and Systems Conference, 2006. IET* (pp. 463-468). IET..

[25] Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011). Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications*, *61*(3), 527-542.

[26] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645-1660.

[27] House, W. (2014). Big data: Seizing opportunities, preserving values. *Washington, DC: Exceutive Office of the President*..

[28] Paul, S., Pan, J., & Jain, R. (2011). Architectures for the future networks and the next generation Internet: A survey. *Computer Communications*, *34*(1), 2-42.

[29] Junaid, M., Akbar, M., & Mufti, M. (2008, December). Per Packet Authentication for IEEE 802.11 wireless LAN. In *Multitopic Conference, 2008. INMIC 2008. IEEE International* (pp. 207-212). IEEE.

[30] Uckelmann, D., Harrison, M., & Michahelles, F. (2011). An architectural approach towards the future internet of things. In *Architecting the internet of things* (pp. 1-24). Springer Berlin Heidelberg.

[31] Santucci, G. (2009, September). Internet of the future and internet of things: what is at stake and how are we getting prepared for them. In *eMatch conference, Oslo*.

[32] Bernat Vercher, J., Perez Marin, S., Gonzalez Lucas, A., Sorribas Mollon, R., Villarrubia Grande, L., Campoy Cervera, L. M., & Hernández Gómez, L. A. (2008). Ubiquitous Sensor Networks in IMS: An Ambient Intelligence Telco Platform..

[33] Korzun, D. G., Balandin, S. I., & Gurtov, A. V. (2013). Deployment of Smart Spaces in Internet of Things: Overview of the design challenges. In *Internet of Things, Smart Spaces, and Next Generation Networking* (pp. 48-59). Springer Berlin Heidelberg.

[34] Cardone, G., Corradi, A., & Foschini, L. (2011). Cross-network opportunistic collection of urgent data in wireless sensor networks. *The Computer Journal*, bxr043.

[35] Lin, H., Wang, L., & Kong, R. (2015). Energy Efficient Clustering Protocol for Large-Scale Sensor Networks. *IEEE Sensors Journal*, *15*(12), 7150-7160.

[36] Ye, W., Heidemann, J., & Estrin, D. (2004). Medium access control with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Transactions on networking*, *12*(3), 493-506.

[37] Li, F., & Xiong, P. (2013). Practical secure communication for integrating wireless sensor networks into the internet of things. *IEEE Sensors Journal*, *13*(10), 3677-3684.

[38] Bluetooth, S. I. G. (2010). The bluetooth core specification, v4. 0. *Bluetooth SIG: San Jose, CA, USA*.

[39] Schulcz, R., & Varga, G. (2011). Radio frequency identification. *Advanced Communication Protocol Technologies: Solutions, Methods, and Applications*, 502-526.

[40] Herberg, U., & Clausen, T. (2011). Study of multipoint-to-point and broadcast traffic performance in the "IPv6 Routing Protocol for Low Power and Lossy Networks". *Journal of Ambient Intelligence and Humanized Computing*, *2*(4), 293-305.

[41] Specification, Z. v1. 0: ZigBee Specification (2005). *San Ramon, CA, USA: ZigBee Alliance*.

[42] Cardone, G., Corradi, A., & Foschini, L. (2011). Cross-network opportunistic collection of urgent data in wireless sensor networks. *The Computer Journal*, bxr043.

[43] Gnawali, O., Fonseca, R., Jamieson, K., Moss, D., & Levis, P. (2009, November). Collection tree protocol. In *Proceedings of the 7th ACM conference on embedded networked sensor systems* (pp. 1-14). ACM.

[44] Jun, Z., Simplot-Ryl, D., Bisdikian, C., & Mouftah, H. T. (2011). The internet of things. *IEEE Commun. Mag*, *49*(11), 30-31.

[45] Yarvis, M., Kushalnagar, N., Singh, H., Rangarajan, A., Liu, Y., & Singh, S. (2005, March). Exploiting heterogeneity in sensor networks. In *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.* (Vol. 2, pp. 878-890). IEEE.

[46] Fremantle, P., & Scott, P. (2015). A security survey of middleware for the Internet of Things. *PeerJ PrePrints*, *3*, e1521.

[47] Vieira, M. A. M., Coelho, C. N., da Silva, D. C., & da Mata, J. M. (2003, September). Survey on wireless sensor network devices. In *Emerging Technologies and Factory Automation, 2003. Proceedings. ETFA'03. IEEE Conference* (Vol. 1, pp. 537-544). IEEE.

[48] Chakravorty, R., Cartwright, J., & Pratt, I. (2002, November). Practical experience with TCP over GPRS. In *Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE* (Vol. 2, pp. 1678-1682). IEEE.

[49] Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497-1516.

[50] Wainer, J., Campos, C. J. R., Salinas, M. D. U., & Sigulem, D. (2008). Security requirements for a lifelong electronic health record system: An opinion. *The open medical informatics journal*, *2*, 160.

[51] Dehling, T., & Sunyaev, A. (2014, January). Information Security and Privacy of Patient-Centered Health IT Services: What Needs to Be Done?. In *2014 47th Hawaii International Conference on System Sciences* (pp. 2984-2993). IEEE.

[52] Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering–a systematic literature review. *Information and software technology*, *51*(1), 7-15.

[53] de Almeida Biolchini, J. C., Mian, P. G., Natali, A. C. C., Conte, T. U., & Travassos, G. H. (2007). Scientific research ontology to support systematic review in software engineering. *Advanced Engineering Informatics*, *21*(2), 133-151.

[54] Bogale, H. Y., & Ahmed, Z. (2011). A Framework for Security Requirements: Security Requirements Categorization and Misuse Cases.

[55] Hannay, J. E., Sjoberg, D. I., & Dyba, T. (2007). A systematic review of theory use in software engineering experiments. *IEEE transactions on Software Engineering*, *33*(2), 87-107.

[56] Glaser, B. G., & Strauss, A. L. (2009). *The discovery of grounded theory: Strategies for qualitative research*. Transaction publishers.

[57] Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches*. Sage.

[58] Carver, J. (2007). The use of grounded theory in empirical software engineering. In *Empirical Software Engineering Issues. Critical Assessment and Future Directions* (pp. 42-42). Springer Berlin Heidelberg.

[59] Corbin, J., & Strauss, A. (2014). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications.

[60] Charmaz, K. (2006). Constructing grounded theory: A practical guide through qualitative analysis (Introducing Qualitative Methods Series).

[61] Bamasag, O. O., & Youcef-Toumi, K. (2015, October). Towards Continuous Authentication in Internet of Things Based on Secret Sharing Scheme. In *Proceedings of the WESS'15: Workshop on Embedded Systems Security* (p. 1). ACM.

[62] Greensmith, J. (2015, July). Securing the Internet of Things with Responsive Artificial Immune Systems. In *Proceedings of the 2015 Annual Conference on Genetic and Evolutionary Computation* (pp. 113-120). ACM.

[63] Horrow, S., & Sardana, A. (2012, August). Identity management framework for cloud based internet of things. In *Proceedings of the First International Conference on Security of Internet of Things* (pp. 200-203). ACM.

[64] Hwang, Y. H. (2015, April). Iot security & privacy: threats and challenges. In *Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security* (pp. 1-1). ACM.

[65] Kanuparthi, A., Karri, R., & Addepalli, S. (2013, November). Hardware and embedded security in the context of internet of things. In *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles* (pp. 61-64). ACM..

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

[67] Yang, K., Forte, D., & Tehranipoor, M. M. (2015, November). Protecting Endpoint Devices in IoT Supply Chain. In *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design* (pp. 351-356). IEEE Press.

[68] Christin, D., Reinhardt, A., Mogre, P. S., & Steinmetz, R. (2009). Wireless sensor networks and the internet of things: selected challenges. *Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose Sensornetze*, 31-34.

[69] Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*, *7*(12), 2728-2742..

[70] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. *Wireless Networks*, *20*(8), 2481-2501.

[71] Van Kranenburg, R., & Bassi, A. (2012). IoT challenges. *Communications in Mobile Computing*, *1*(1), 1.

[72] Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*, *17*(2), 261-274.

[73] Polk, T., & Turner, S. (2011, February). Security challenges for the internet of things. In *Workshop on Interconnecting Smart Objects with the Internet, Prague*.

[74] Keoh, S. L., Kumar, S. S., & Tschofenig, H. (2014). Securing the internet of things: A standardization perspective. *IEEE Internet of Things Journal*, *1*(3), 265-275.

[75] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146-164.

[76] de Leusse, P., Periorellis, P., Dimitrakos, T., & Nair, S. K. (2009, June). Self Managed Security Cell, a security model for the Internet of Things and Services. In *Advances in Future Internet, 2009 First International Conference on* (pp. 47-52). IEEE.

[77] Hancke, G. P., Markantonakis, K., & Mayes, K. E. (2010). Security Challenges for User-Oriented RFID Applications within the" Internet of Things". *網際網路技術學刊*, *11*(3), 307-313.

[78] Chaqfeh, M. A., & Mohamed, N. (2012, May). Challenges in middleware solutions for the internet of things. In *Collaboration Technologies and Systems (CTS), 2012 International Conference on* (pp. 21-26). IEEE.

[79] Coetzee, L., & Eksteen, J. (2011, May). The Internet of Things-promise for the future? An introduction. In *IST-Africa Conference Proceedings, 2011* (pp. 1-9). IEEE.

[80] Vermesan, O., & Friess, P. (Eds.). (2015). *Building the hyperconnected society: Internet of things research and innovation value chains, ecosystems and markets* (Vol. 43). River Publishers.

[81] Zorzi, M., Gluhak, A., Lange, S., & Bassi, A. (2010). From today's intranet of things to a future internet of things: a wireless-and mobility-related view. *IEEE Wireless Communications*, *17*(6), 44-51.

[82] Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realising the Internet of Things. *Cluster of European Research Projects on the Internet of Things, European Commision*.

[83] Gusmeroli, S., Piccione, S., & Rotondi, D. (2012, September). IoT@ Work automation middleware system design and architecture. In *Proceedings of 2012 IEEE 17th International Conference on Emerging Technologies & Factory Automation (ETFA 2012)* (pp. 1-8). IEEE.

[84] Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A vision of IoT: Applications, challenges, and opportunities with china perspective. *IEEE Internet of Things journal*, *1*(4), 349-359.

[85] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

[86] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805..

[87] Ma, J., Wen, J., Huang, R., & Huang, B. (2011). Cyber-individual meets brain informatics. *IEEE Intelligent Systems*, *26*(5), 30-37.

[88] Malakooti, M. V., & Mansourzadeh, N. (2015). A Two Level-Security Model for Cloud Computing based on the Biometric Features and Multi-Level Encryption. In *Islamic Azad University, The Proceedings of the International Conference on Digital Information Processing, Data Mining, and Wireless Communications, Dubai, UAE*.

[89] Bassi, A., Clarke, J., Charles de Couessin, F., Ioannidis, S., Kosta, E., McCarthy, P., ... & Rotter, P. (2010). Flying 2.0 Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology.

[90] Wu, G., Talwar, S., Johnsson, K., Himayat, N., & Johnson, K. D. (2011). M2M: From mobile to embedded internet. *IEEE Communications Magazine*, *49*(4), 36-43.

[91] Moses, L. B. (2007). Recurring dilemmas: The law's race to keep up with technological change. *U. Ill. JL Tech. & Pol'y*, 239.

[92] Council, the N. I., Nic, N., & Intelligence, S. C. B. (2008). Disruptive Civil Technologies Six Technologies With Potential Impacts on US Interests Out to 2025.

[93] Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, September). On technical security issues in cloud computing. In *2009 IEEE International Conference on Cloud Computing* (pp. 109-116).

[94] Ning, H., & Liu, H. (2012). Cyber-physical-social based security architecture for future internet of things. *Advances in Internet of Things*, *2*(01), 1.