International Journal of Innovative Studies in Sciences and Engineering Technology (IJISSET)
ISSN 2455-4863 (Online) **www.ijisset.org** *Volume: 3 Issue: 9 | September 2017*

Research Trends of Network Security in IoT

D Gayitri Aneela[1], I A Anusha[2], K Malavika[3], Dr. Ravi Saripalle[4]

[1]*D Gayitri Aneela, Student, GVP College of Engineering(A), Visakhapatnam, AP*
[2]*I A Anusha, Student, GVP College of Engineering(A), Visakhapatnam, AP*
[3]*K Malavika, Student, GVP College of Engineering(A), Visakhapatnam, AP*
[4]*Dr. Ravi Saripalle, GVP College of Engineering(A), Visakhapatnam, AP*

Abstract: *The technology has been evolving and producing multiple innovations in the last decade. Internet of Things (IoT) is considered as most revolutions in technology. IoT connects two worlds, the virtual and the real. In this paper, we carry out a systematic review of the literature regarding the different considerations, challenges, and threats that have influenced network security in IoT domain. We conducted a keyword-based search on selected databases to identify the articles for systematic review. A total of 712 full-text articles reviewed, and the results revealed the use of several protocols and architectures to secure the Internet of Things. The results also emphasized the inevitability of enhanced network security for IoT. We also discussed future research opportunities in this paper which are expected to stimulate more research in the IoT network security space.*

Keywords: *IoT, Network Security, Internet of Things.*

1. INTRODUCTION

Internet of Things (IoT) denotes a network of physical objects that interconnect through cyberspace as well as the communicative process involved within. The network helps in the transfer of enormous amounts of data between devices without human intervention. Gartner analysis says that by 2016, the use of interconnected things will reach 6.4 billion, 30 times the number of devices connected in 2009. This number will rise to 20.8 billion by the year 2020 as per projection [20]. Many industries now are also finding more and more use of these devices. In fact, there is an increase in the demand of these devices in various disciplines like smart homes, e-health, wearables, manufacturing automation, automobile, supply chain, agricultural farming and other operational technologies. Despite this sudden rise in demand, there are still issues that need addressing regarding the security of these devices. HP conducted a study and found out that about 70 percent of most commonly used Internet of Things (IoT) devices contain vulnerabilities regarding password security, user access permissions, encryption, and more. These threats are mainly Potentially Unwanted Applications (PUAs), Distributed Denial of Service Attacks (DDoS) and other forms [21].

Since IoT devices connect to networks, they need high layers of security shields. For ensuring that the layers are secure, diverse types of protocols, algorithms, security policies and procedures are employed. These measures play important roles in the core security aspects of IoT which is the main concept studied in this paper. Specifically, the present study addresses the following research questions:

•RQ1: What are the major challenges that have guided security in IoT?

•RQ2: What are the critical solutions and trends in IoT bound network security?

The article is structured as follows: Section 2 describes the research process in detail. Section 3 covers the findings based on the review which in turn is the main discussion in the Section 4. The summary of our contributions as well as a discussion on the limitations of the study is discussed in Section 5.

2. RESEARCH APPROACH

2.1. Research Overview

We used a non-experimental take to the study through content analysis to do a systematic review addressing the research questions proposed above. The content analysis helps provide a structured and systematic approach to classifying and describing the text materials on the current literature. [4]. In this paper, we refined the text materials via a spreadsheet containing categories and sub-categories to classify the key components from the text materials that will serve as suitable evidence. We listed down our observations and the discussion of our findings from the observations are in Sections 3 and 4 of this article.

2.2. Classification Framework

In this paper, we implemented the suggested methods from Higgins and Green [5], and Kitchenham et al., [6] for the systematic review of classification guidelines. The codebook contains six descriptors i.e. year, journal or conference, title, volume no, doi), author keywords, associated SDLC Phase, security phase relevancy, and security-related key terms [22].

2.3. Data Collection

We searched the databases of ACM Digital Library, IEEE Xplore, Springer, ScienceDirect, and Wiley InterScience through keyword-based search [22]. The search keyword is 'IoT and NETWORK SECURITY' in 'AND' format to select the text materials or articles for analysis. The used search string applied to Full Text & Metadata. The process took place in the months of November and December, the year 2016. We omitted standards, editorials, courses, tutorials, prefaces, workshops, poster sessions, and other English language articles in the search process.

The 2906 matches recited in Table 1 contain duplicates as there are text materials or articles that are pulled up during the search of the databases used. We did further filtration of the pulled articles to gauge the appropriateness of use. To detect exclusion, we considered the relevance of the article to IoT and Network security domain.

TABLE 1: *Database Search Results*

Data Bases (Journals and Conferences)	No of Hits
IEEE Xplore	729
ScienceDirect	951
ACM Digital Library	113
Springer Link	725
Wiley InterScience	388
Total	2906

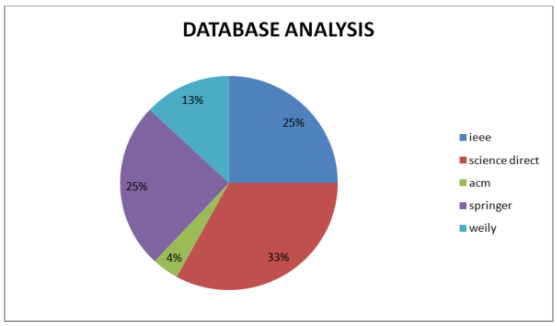

Figure 1: *Journal Database Analysis*

Based on the refined results, we shortlisted 712 credible articles address an issue related to Network Security for IoT.

3. FINDINGS

We systematically reviewed 712 articles that resulted from the selection process conducted on the chosen databases. Out of the 712, 627 articles are academic journals, five are books, and 80 are conference proceedings. From the 712 articles, there are 169 which are papers published between 2010 and 2013, 535 are publications between 2014 and 2016 (both years inclusive), and eight articles are between 1983 and 2009. Given the number of publications per year range, it is evident that the interest and emphasis on the security in IoT increased in the last three years with an exponential difference as compared to previous years. With these findings, we now address the research questions and corresponding responses.

RQ1: What are the major challenges that have guided security in IoT?

In this paper, we identified fundamental security challenges related to highly dynamic IoT networks and highlighted network characteristics. We found out that any IoT device is expected to be well secured and reliable to meet the privacy criteria, especially when these devices work in conjunction with applications such as defense, medical sciences, automobile, etc., where the role of security is a chief concern. However, due to the small size of these IoT devices, they have very low computational capabilities which make it difficult to cover security [7]. Because of the liabilities in securing these devices, attacks such as Eavesdropping, Trojans, Denial of Service Phishing, IP spoofing, and a lot more, become critical subjects to study in the context of IoT security. The limited power of these IoT devices also makes it difficult to design an efficient architecture for networking of sensors and storage of data.

RQ2: What are the critical solutions and trends in IoT bound network security?

For ensuring the security of the Internet of Things, a division of these things into groups as "communities" can be employed. Furthermore, these communities can communicate with each other when there is appropriate authorization [1]. Because of this, the transfer of data is perilous. Hence, the security of the data traffic between the devices and the cloud must be a high priority. There are a lot of methods available to enforce security to the data. There are encryption techniques such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). There are also

protocols like Secure Mesh which is the one used in Ambient Assisted Living (AAL), particularly relating to eHealthcare [2], a lightweight defensive algorithm for the DDoS attack [3], layered wireless protocols (Network/Communication, PHY/MAC, and Application layer). The network/communication layer includes IPv6/IPv4, TCP/UDP, and 6LoWPAN. The PHY/MAC layer includes 802.X series, WirelessHART, UWB, IrDA, and PLC. The application layer includes CoAP, SNMP, DNS, and DLMS [19].

There are many security solutions available for network devices, but the 802.15.4 link-layer security is the current popular method. If data integrity is in question, the 6LoWPAN network is go-to since it can support per hop security arrangements by using symmetric key cryptographic devices. With this network, there is an assurance of confidential functioning, source authentication, replay security, data fusion, and semantic protection. The network also grants direct access to the web using open standards. When it comes to the security of the network, the IP Security (IPSec) protocols are embedded into TCP/IP protocol stack via software in the OS used, such as Linux and NetBSD. However, the protocol is quite computationally intensive [18], which greatly affects the performance of the network [9]. [8]. Before, web transfer or web access relies on the application layer CoAP protocol which allows web transfer with constrained nodes and networks. This protocol integrates security modes such as NoSec, PreShared-Key, RawPublicKey, and Certificate which is proven valuable in securing the transport layer. However, CoAP is still less secure which puts data integrity in question especially against DDoS attacks. Hence, the Datagram Transport Layer Security (DTLS) is integrated to attain the authenticity, confidentiality, and integrity required. The protection is achieved via cookies in the web protocol domain [10]. Usually, there is a set of application protocols implemented. One popular set used is the ZigBee, based on the IEEE 802.15.4 PHY and MAC sublayer. The protocol set can create effective and efficient mesh networks that can link to up to 216 devices. These mesh networks are proven energy-efficient, have low data-rate and are self-configuring.

In all the above protocols, metadata, including source and destination addresses, are sent between nodes which are highly susceptible to a range of attacks primarily based on eavesdropping and packet injection. For more control over the process and measurement environment, the WirelessHART protocol is useful. The protocol is robust and reliable with above 99.73% availability ratio thanks to the TDMA-based MAC sublayer integrated within using TSMP technology. There are still limitations with the security architecture which needs addressing. [11].

Questions on network access authenticity on the architecture is addressable by using the Protocol for Carrying Authentication for Network Access (PANA), a network layer protocol used to enable authenticated access to the network. It is UDP-based EAP and runs between an EAP peer and an EAP authenticator [12].

A high-performance, ultra-lightweight, deep-packet anomaly detection approach that runs on small IoT devices are also go-to. The approach utilizes n-gram bit-patterns to efficiently and flexibly model payloads which allow the n-gram size to vary by dimension. [13]. to achieve the lightweight integration, Elliptic Curve Cryptography (ECC) is ideal for building up lightweight Public Key Cryptosystems (PKC). It is mainly because of the small key size, small operand length, and comparably low arithmetic requirements of the system [14]. For the Black Network, similar control over the security of the communication and network transfer pathway is achievable through Black SDN, an IoT network architecture that utilizes an SDN controller as the trusted-third-party link. Encrypting the header and the payload to mitigate a range of attacks is one surefire method. [15]. To bring all these network functions and protocol information, as well information identifiers to the core of the system, the ICN, a new (inter-) networking paradigm, is used. The ICN is most favorable because of its flexibility regarding information retrieval. ICN allows information “advertisement” and “retrieval” through flexible semantic-rich identifiers. It is different from location-dependent identifiers, such as IP addresses [16].

In this research, we concisely reviewed security in IoT and analyzed security characteristics and requirements from different layers. Based on the findings, it is possible that by developing the Internet of Things, more security problems may arise.

4. DISCUSSIONS

In this section, we discuss the results of our systematic review of the 712 articles selected about Network security in IoT. As analyzed, the objective in most of the articles has been to attain a way to convey Network security in IoT devices. This paper follows the positivistic paradigm that studies the facts which are

observable and classifiable. The articles reviewed which used qualitative research methodology in finding the results focused on achieving Network security in IoT. There are also a few cases where both the qualitative and quantitative methods are notable. These articles made use of both approaches to determine efficient algorithms, architecture, and protocols.

We also take note that with articles relating to Network security in IoT, the primary approach is to use experimental research. The main purpose of the approach has been to uncover various Network security threats and attacks. The employment of case study analysis as a research strategy is also notable, wherein specific settings are selected to address issues relating to Network security in IoT for example [17].

Regarding the article distribution, more than half of those centered on Network security in IoT are publications since 2010. This increase in the number of articles published is a seemly evidence of how the domain is gaining interest from researchers all over the world. The reason for such increased interest could be because of the growing complexities of systems, heterogeneous business scenarios, and a highly competitive and vibrant marketplace to operate, survive and sustain. We found that most of the articles have focused on rendering security for IoT. The traditional methods are fading in the face of more advanced methods which make IoT devices more secure.

The following limitations were also noted for this study:

- Use of differing keywords for the search may lead to different findings. Hence, the keywords were chosen to provide a focused overview of current trends in the Network security in IoT.
- Using the same keyword when searching in similar libraries at a different date could generate different findings (e.g., due to a search engine used or library updates).

5. CONCLUSIONS

Network security plays a vital role in IoT. This vitality in the role is especially imminent due to how the security implications became more proclaimed after the increase in the radicality of the impact of attacks. It can be because of how IoT includes a wide range of applications. Few of the key challenges for IoT that is of high concern today include security, privacy, and confidentiality, management of heterogeneities, limitations of network capacities, management, and processing of massive quantities of data to provide useful information. In this paper, we examined different interests that have influenced Network security in IoT to date. We based our analysis on the results of the systematic review that we conducted on selected text materials and articles to address our research questions. Our findings posit that the number of contributions to ensure the security of IoT devices in recent years has increased and that there are different considerations of levels of security. The use of standard protocols in the IoT affords interoperable communication between constrained IoT devices and services.

The study has limitations that need consideration. The relevance of the articles that we have included in the systematic review can still be subject to questioning. The manner as to how the databases and conference proceedings selection process went through in regards to our systematic review still needs more tweaking. A bias analysis result of the selection of articles or text materials can still be possible because of the specific objectives and aims. There is also an undeniable possibility that the results attained by using the search string 'IoT AND NETWORK SECURITY' in specified channels could prove as non-exhaustive. There may be articles which might not get identified in the search as the term "IoT" and the term "NETWORK SECURITY" are not the identifiers or part of used for the retrieval.

There can be further research done with a focus on the possible increase in consideration of external concerns of Network security in IoT. The driving principle could be the fact that there has been an increased emphasis on various levels of security. Additionally, attention towards business considerations is one of the external factors for considering security in IoT which is also a great context for further study. All these possibilities are expected to encourage researchers to join in this line of inquiry and research.

REFERENCES

[1] D. T. Bui et al., "Supporting multicast and broadcast traffic for groups of connected devices," (2016), pp .48-52.

[2] F. Augusto Teixeira et al. "Defending Internet of Things against Exploits," vol 13, (2015), pp. 1112-1119.

[3] C. Zhang and R. Green, "Communication security in internet of thing: Preventive measure and avoid DDoS attack over IoT network

[4] B. Downe-Wamboldt, "Content analysis: Method, applications, and issues," *Healthcare for Women International*, vol. 13, (1992), pp. 313-321.

[5] J. P. T. Higgins and S. Green, "Cochrane handbook for systematic reviews of interventions (version 5.1. 0)," *The Cochrane Collaboration*, (2011).

[6] B. Kitchenham et al., "Systematic literature reviews in software engineering: A tertiary study," *Information and Software Technology*, vol. 52, (2010), pp. 792-805.

[7] S. Koley and P. Ghosal, "Addressing hardware security challenges in internet of things: Recent trends and possible solutions," (2015), pp.517-520

[8] G. Lessa dos Santos et al., "A DTLS-based security architecture for the internet of things," (2015), pp.809-815.

[9] M. Rao et al., "FPGA-based reconfigurable IPSec AH core suitable for IoT applications, (2015), pp.2212-2216.

[10] D. Singh et al., "Secure layers based architecture for internet of things, (2015), pp.321-326.

[11] S. Chakrabarty et al., "Black SDN for the internet of things," (2015), pp. 190-198.

[12] J. L. Hernandez-Ramos et al., "Dynamic security credentials PANA-based provisioning for IoT smart objects," (2015), pp. 783-788.

[13] D. H. Summerville et al., "Ultra-lightweight deep packet anomaly detection for internet of things devices," (2015), pp.1-8.

[14] Z. Liu et al., "On emerging family of elliptic curves to secure internet of things: ECC comes of age," vol (pp-99), (2016), pp. 1-1.

[15] S. Chakrabarty et al., "Black SDN for the internet of things," (2015), pp.190-198.

[16] Y. Chen et al., "Timed-pNets: A communication behavioural semantic model for distributed systems," *Multimedia Tools and Applications*, vol. 73, (2014), issue 2

[17] Y. Nizami and E. Garcia-Palacios, "Internet of things a proposed secured network topology," (2014), pp.274-279.

[18] A. Ferrante et al., "IPSec hardware resource requirements evaluation," *Next Generation Internet Networks (NGI 2005)*, April 2005. pp.240-246, doi: [10.1109/NGI.2005.1431672]

[19] V. Gupta et al., "Sizzle: A standards-based end-to-end security architecture for the embedded internet," in *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*, March 2005, pp. 247–256.

[20] R. van der Meulen. (2015, November 10). *Gartner* [Online]. Available: http://www.gartner.com/newsroom/id/3165317

[21] K. Rawlinson. (2014, July 29). *HP* [Online]. Available: http://www8.hp.com/in/en/hp-news/press-release.html?id=1744676

[22] R. Thakurta. "Research trends on software requirement prioritization," *International Journal of Software Engineering and Its Applications*, (2014), vol. 8 (6), pp. 287-298