LITERATURE SURVEY ON INTERNET OF THINGS (IOT) IN HEALTHCARE SYSTEMS USING SECURITY MECHANISMS, CYBER DISCUSSIONS AND PRIORITY PROTOCOLS

*G. Angeline Prasanna *, Krishna Priya*

Abstract

IoT, Internet of things can better be referred as a field where we are discussing of smart titled things which includes the altogether concept of, where smart cities, smart homes, smart industries and what not for the industry revolution 4.0. And to that technology being existing as wired and wireless networks and a combination of topologies for the infrastructure. Being security mechanisms a common breach now, it cannot be compromised with the health and the single "physical unit" of all invention-Man who is behind the finding and also the breaches.so healthcare needs more security mechanisms both in areas of algorithms and techniques as well as tools are being studied through various papers mentioned below.

Keywords: Industry4.0, security breach, wireless networks.

I. INTRODUCTION

Internet of things is the giant topic branched and the independent centralized system of working with networks with the adapted network concept which will help a person get anything from internet if he or she can name it.

Network itself is a vast area, which is the collection of systems, hosts, and changing roles of clients and servers.

The importance and role of protocols cannot be disregarded, technology and techniques implied for implementing security features is a must discussed topic for connected environment which is the ongoing era, that with the connection zika billion devices in the networks, Security is the most sought out topic under discussion. Internet of Things (IoT), which joins and webs the network of smart devices which will serve and do the surveillance within the healthcare systems connected being e-bands, tags, healthcare databases which are confidential in nature according to the technology which joined them further specialising to areas of medical Iots. Due to its nature to ever time modifiable and confidential information of patients is to be an area which needs inurement of security as a critical issue in the development of IoT-based healthcare system and the related domains and protocols proposed

The identification process and the features, concepts associated with security requirements of IoT in healthcare system is a broad area which cannot compromise neither on integrity and accountability of data been transferred through devices which has now reached the stage of wireless body area networks(WBAN).The cyber studies have shown that the requirements in cyber space is too big to Cyber security requirements are divided into two parts: CIA T (three features) and non-CIA (seven features) spectrum. Both traditional (cyber security) and breach out detection and devise-based requirements should be taken into consideration in order to achieve the complete secure network architecture and skeletal outline of data transferred between layers of ISO OSI & TCP/IP levels in IoT-based healthcare system also for the offending and defending processes.

II. LITERATURE SURVEY

1.Dia M. Ali, Department of comm and electronics, Nineveh, Mosul/Iraq, Ahmed S Mahmoud, Electronics and communication, College of engineering, Mosul,

Department of Computer Applications,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
*Corresponding Author

IoT security Assessment in Healthcare Environment [1]. IoT security Assessment in Healthcare system.

Internet of Things (IoT) can be referred according to the paper as a customised design of or in other words the topological framework of physically connected sensor-based devices forming in to a finalised network.it contains the built-in technology where the sensors are communicating as the protocol transmissions with both internal and external IoT, The environmental issues are also well taken care of, Any how the new buzzword of today's technological niche the terminology of integrating machines and networks for surveillance process and monitoring devices are there in the plan and action of many men and countries since years and they are just refreshing it with the ideas of advancement in in wireless technological areas of Machine to Machine, machine to man as Stephen hawking said we are all interrelated and communication happens as neurons of a brain and DNA, MONACO molecular networks [2] studies are all new branches sprouting as the support system and inventions are happening in these fields with the connected facility provided by internet of things[3] where ventures as well diligence diagnostics for perimeter based surveillance.

METHODOLOGY

The paper details with the cohort of cyber space devices that is presently named as Internet of Things or the net and more concerning the health care management systems. That web area of health sector and hospital management allows comprehending the devices connected amongst themselves, where because of this interconnection they suffer outbreaks of threats over the vulnerabilities in a network and when referring to these again the point which becomes valid is with the lives of the many ranging from the rags to riches, because people matter to places as well as to countries.

The alternate option or a logical method to apply is with encryption techniques and masking techniques passing over the internet. The coders of the passwords and the decoders of the data are ciphering it in a way that the plain text is moulded in particular pattern that peeping to it cannot assume or guess the content of the data wrapped in it. Here the discussions go as such there are brokers [4] or third parties where the content encapsulation and polymorphic texts are generated between the sender location which usually will be the home server and with today's terminology of cloud storage [5] and all, it reaches to the cloud servers for the particular. The result as such gives the assurance on the intermediate security for the wide range of applications that is to be operated with it.

The new cryptographic technology [6] related with irreversible storage base where the concept is having a secret and hidden key for transmission of the message from the beginning of a sensor end or a port to its endpoint within the given period of time [7]. Advantage defined with the method is to reduce complexity and transfer safe as far as possible in the internet of things [8].

Sec Rout Protocol

The protocol design is as such each node will be having the structure as per the plan the topological network structure is classified into clusters that have heads and to each head cluster, self-alignment and the identified sensor node recognises the cluster's master or the head node [8].

The architecture details the parallel and partial route which includes the data also the details of routing packets, in the table which is usually small in number. As the nodes gets integrated the in-between nodes recognises its route acceptance, a new concept other than source routing is used. AODV Protocol is the idea introduced so has to go with its two phases, one being discovery of route phase and the second being maintenance of route phase [9]. Here a source node will not be possessing no route information and the functionality remains with the transmission of a data packet to the destination port. The route discovery thus deals with the traversal routes of a node. The node which initiates will send a route request RREQ by broadcasting the data with a unique ID so as to stop hoping in route.

The time when a RREQ request [10] is reached to the neighbour node, that then connects to a route which will exists as the temporary one to the end point, and is returned to the source for the reply as a method of the old handshake connection. This is transferred into the neighbouring nodes through a RREQ.The end which accepts the RERP information forms the route to route for sending the information from source to the destination node. The node detects the source part and checks whether valid or not. It keeps alive the procedure into cracked parts where the computing route responding a RERR packet to neighbour nodes that repeats the procedure. Later the process is repeated to as many nodes in the table for transmission of data from the sender to the destination [11].

2. Somayeh Nasiri1, Farahnaz Sadoughi2, Mohammad Hesam Tadayon3, Afsaneh Dehnad4

Security Requirements of IoT based Healthcare systems [12]

The IoT terminology shared where the contemporary ideas are given by Kevin Ashton during 1999. Where the concept connects innumerable number of devices together that no simulation or machinery support is further needed from the human side once connected to the network. The mobile data transmissions and cloud storage of today will ensure and visualises the reality and virtual gap between the world and connection with internet[13].IoT powers over the all sustainable, life supporting ,economic areas of a nation including its prestigious glamour for agriculture, healthcare, smart cities ,logistics to automated vehicles in the mini list taken[14].it relates not only to the ambient assisted living AAL but also with the health care in diagnosing the diseases earlier and monitoring it without interruption. It is thus found to be the best fitness support [15] program at the earlier stage and support for the elderly [15][16].

METHODOLOGY

The applications and advantage over that will be innumerable but the sensitive data of the patient related with the medical systems [17] are the prone areas of vulnerability-based attacks,

The IoT attack [18] may vary from complicated to life threatening, the implant givers and medical device manufacturers of medical IoT devices often neglect the issues and risks of security levels. And thus, stressing with the keyword terminologies of integrity [19], confidentiality, accountability becomes the point of discussion and importance.

Thus, the [20] compromise over medical devices is outdated and proper monitoring is done over the titles of privacy, security, and integrity of the health care devices and its transmissions.

3. Ria Das, Indrajit Das

Secure Data Transfer in IoT environment: adopting both Cryptography & Steganography techniques [21]

The IoT framework outlines the story part as the networking, computing of best paths or routes, storage botheration, the connection modes, the connection architecture, the loop holes left over. The supporting factors being sensors, objects, sensor- embedded smart devices and also the commonly used devices of a common house or an office. The idea is to support, generate, transmit, communicate and consume without storage and human support systems [22]. To describe it in a more judicial and intellectual way it is a compound of inseparable collaboration of many hardware and software things put together, where the acronym any can be mixed with time, place and what not as a wish you can name. To sum up as just a beginning of a spark where the flame and fire is left over with this fantastic sought out architecture of IoT in a way such that, how thoroughgoing was the impact that a person gets connected to a system especially because of the network as per the statistics taken entitled to smart devices [23].

METHODOLOGY

As per the positioned status of IoT devices, the numbers give the hoping alarms of the devices which is about to get doubled in the upcoming years in trillions as per the annual reports of network giants of the world. Many surveys are conducted including siemens, IBM, cisco [23], the network giants of the world, the specimens shows that the IoT applications has the succeeding years with e-health-finance and e-cities to say. There are top threats found out with the study as targets [24].

Along with the advent of a new technological functioning came the ticklish question whether the security [25] is met to the necessity and to the unexpected at the unexpected times and which, when is the exact time of a security breach.

To say the supplied throughout and diversified character of IoT connected objects integrated together with adequate security measures paved the way to jeopardised condition of cyber security breakups as per the observation. Eavesdropping, peeping up, Sniffing, whaling and masquerading are the many among the list of breaches happened. The technique of wrapping up of confidential data via texts and images where the secret data gets hidden inside is known by the name steganography.

Cryptography technique [26][27] cannot stop the exposure of data from the attacker's line drawn virtually.as sensors are the major workable units embedded in the IoT devices which is the vulnerable point, employers need to make sure whether proper configuration checks are done with the processing part, limited memory area, and the cryptographic technique's security with the power of algorithm used for various orders. Thus, Lightweight cryptography is the area specialised for the cases where the niches like hospital and healthcare devices, smart car like upcoming IoTs having RFID tags use an algorithm where number of code length is less and the RAM size also. The special highlights of this methods are higher end to end communication with great effectiveness and durability with less complications as per the study. Again, when it comes to the limitations are with the less and decreasing encryptions rounds with the bits and reduced length with the key size [28]. As the common cryptographic classifications, the cryptographic techniques are of symmetric and asymmetric in nature. The light weight cryptography [29] also follows the same. The communicating ends use a shared key and common key, where the common key is used for doing both encryption and decryption. In symmetric, whereas asymmetric is a bit detail to know better after analysing the examples of symmetric [30]. In the list of symmetric light weight encryption examples:

1.XOR 2. PRESENT,3. HIGHT,4. AES,5.CS,6. SCA etc can be mentioned.

In relation with the XOR operation, a lightweight protocol [30] is suggested with the concept of RFID tags so as to confirm the working. The quixotic part of the work to the concept of researchers is design with the latest finger print device design and the system-based chip embedded in the microcontroller with the IEEE 802.15.4 and AES algorithm [31]. Where the finger print analysis will be limited when the person to be subjected is having injured or impure hands [32] for eaves droppers, as per CC2530[33] the received signal strength indicators will have the key distribution and, user's fingerprint feature information detection to perform the extraction and distribution.

The asymmetric cryptography working, it consists of a public key [34] familiar to all, a private key which is only familiar to the specified Port which is the destination node. The public key is usually sent by the receiver to encrypt the data, the receiver's private key is used for decrypting data [35].

Examples of Elliptic Curve Cryptosystem (ECC) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE). There happens the encryption technique with CP-ABE [36] is able to analyse entities that needs to be accessed for data. Many proposed techniques are under research, where Cooperative Ciphertext-Policy Attribute-Based Encryption is adopted to further enhance security of CP-ABE encryption.

4. Sundeep Selvaraj Pundamale Department of Computer Science

Survivable networks [37]

Day by day the network devices get added the global internet and survivable networks is efficiently proven to be more efficient in nature, but the administration is as of central and more complex with the overlapped network architecture [38].

various definition of sustainability is referred as maintenance of several feature-based attributes, the attributes being performance, security, reliability, availability, fault- tolerance also in the list modifiability [38]. Capacity of a system is the potential to output the required and expected services. The functional and design features and working needs is to be met. The capacity is measured in its independent status to survive the threats against vulnerabilities as well the information with a specific clause, computation and communication clause. The feature in the list to lookout for the further approval of security is with the services and properties of functions associated with. The service is finding in terms of accuracy and the reach without any loss of hop is by finding the path or route even in the case of root/node failures and the adaptation to that. It varies with application or areas of specialization when it is to be explained with the military powers or connections the superior order commands to possessing the confidential and integrity of messages transferred through nodes under the maintenance [39] of technical superiors of that particular applicable area.

METHODOLOGY

Network structure of various security self-features associated in the methodology [40].

When to say something is self-aware, it is the ability best described with the management itself without assistance. Where the facilitating functions not only relies with the management and assistance like features of network but also the interruption free facility enclosed with it.

There are again four points discussed with utmost care and considered as the measurement units or features for a self-sufficient network.

self-configuration: The ability of the system to configure automatically with some high-level policies.

Self-optimization is the potential of a system to accelerate the system performance and also the performance of the sub and minor components related with it automatically.

Self-Healing, whereas can be referred as the self patching up features in built in it so as to defend the maximum, detect when attacked, diagnose the particular type of interruption occurred and treat for the repair both with the tangible and intangible parts of a system.

Self-Protection is perfectly explained as the ability of a system to be alert with the precautionary methods and alarm for, when attacks are happened, the alarms can either be as a warning message through alert boxes with frequent occurrences to the sight of a user.

5. Svetlana Budko, Norwegian Computing Centre Habtamu Abie, Oslo, Norway, Adaptive Cyber Security Framework for Health Care IoT [41]

As per the above papers study, the e- health networks are under the surveillance of many directive boards of network and the related associations, so it is high time to look in to the matters where cyber space's critical area of access will be hospital networks and healthcare management systems, officially carried out to the outsiders view with the technological advancements and monitoring and thus data beyond expected are being surveyed with out any authenticity and confidentiality is totally exploited and sometimes the data repositories are knock out with the modified data being damaged with the integrity part.

METHODOLOGY

The computational intelligent society alarms of the threat that can be related with the emerging areas of cyber physical systems and the security related to it. It warns how metamorphic developments in the areas with the computation and security [40] [41] transformation can be reverse engineered for the security to the systems itself as a counter method.

The study further elaborates that the system's property to stand as a dependent and independent system functioning is the main cause where the interconnection can be the chain reaction for the vulnerability spread and the flow of failure issue with one node to the other or an error with the route as part of the inter connection with the topology layout and infrastructure-based working. The aggregative and lively studies show the results summarising and concludes for the above said failure interventions.

With the summary of the cause study, next comes the researchers' study with the understanding of mechanisms that can be put forward to limit the issues and further attacks, it justifies with previous attacks and studies show that traditional methods cannot single handed solve these, rather intelligent and innovative ideas need to be put together so as to tackle these.

A framework for designing resilient distributed intrusion detection systems for critical infrastructures is introduced in [42] the architectures.

The game-theory approach is one particular case of simulation-based attacks and the threats related components, where protection with e-health networks is estimated. This particular showed that the suggested methods are functioning well with the attacks simulated and better mechanisms are also suggested with the game-theory approach.

Ensuing years are of the machines monitoring rather man, the detailed understanding and conclusions are to be derived from the man, then only it can be fed as inputs to the machine, which decides the action to be performed.

Through the gaming simulations and statistical data collected with the data science areas and all we can believe that a better world of new measurements unlearned relearn understandings of intelligent thoughts welcomed over traditional approaches where cyber data security, physical cyber systems, threats to even the machine learned robots needs to be self sufficient and sustainable of the attacks mentioned above and the attacks which is to be appeared in the research study papers of tomorrow.

III. CONCLUSION

Having gone and analysed the discussions of wireless sensor network moulding to IoT transformations, various assessments will be required especially during the cyber security breach era and packet transmissions needs to be monitored with the traffic where exploitation of networks and network devices are happening including monitored and unmonitored still connected environment through penetration testing like tools, Both offensive and defensive areas with the tools and precision study for better priority based protocols are also carried out.so as to hinder the e-breaches or to limit them, Still the breaches also grow together with the added device to the network every second.

REFERENCES

1] Deogirikar J, Vidhate A. Security attacks in IoT: A survey. Proceed- ing of 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). 2017 Feb 10-11; Palladam, India. IEEE; 2017: 32-37.

[2] Dr. Angeline Prasanna G 1, Krishnapriya M, Journal of the Gujarat Research society, ISSN:0374-8588. The Internet of Things, A novel Paradigm for various fields. Volume 21 issue, 17 December 2019.

[3] Islam SMR, Kwak D, Kabir MH, Hossain M, Kwak KS. The Inter- net of Things for Health Care: A Comprehensive Survey. IEEE Ac- cess. 2015; 3: 678-708.

[4] Gholamhosseini L, Sadoughi F, Ahmadi H, Safaei A. Health Inter- net of Things: Strengths, Weakness, Opportunity, and Threats. Proceeding of 2019 5th International Conference on Web Research (ICWR). 24-25 April 2019; Tehran, Iran. IEEE; 2019: 287-296.

[5] Strielkina A, Kharchenko V, Uzun D. Availability models for healthcare IoT systems: Classification and research considering attacks on vulnerabilities. Proceeding of 2018 IEEE 9th Interna- tional Conference on Dependable Systems, Services and Technol-ogies (DESSERT). 2018 May 24-27; Kiev, Ukraine. IEEE; 2018: 58- 62.

[6] Jaghirdar FT, Rudolph C, Bain C, Acm. Can I Trust the Data I See? A Physician's Concern on Medical Data in IoT Health Architectures. Proceeding of Proceedings of the Australasian Computer Science Week Multiconference. 2019 Jan 29-31; Sydney, NSW, Australia. New York: Association for Computing Machinery (ACM); 2019: 1-10.

[7] Alsubaei F, Shiva S, Abuhussein A. Security and Privacy in the In- ternet of Medical Things: Taxonomy and Risk Assessment. Pro- ceeding of 2017 Ieee 42nd Conference on Local Computer Net- works Workshops. 2017 Oct 9; Singapore, Singapore IEEE; 2017: 112-120.

[8] Lu Y, Da Xu L. Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. IEEE Internet Things J. 2018; 6(2): 2103-2115.

[9] Karen Rose, Scott Eldridge, Lyman Chapin, "The Internet of Things: An Overview; Understanding the Issues and Challenges of a More Connected World", The Internet Society (ISOC), October 2015.

[10] M. Katagi and S. Moriai, "Lightweight cryptography for the internet of things," Sony Corporation, pp. 7-10, 2008.

[11] T. Bhattasali, "LICRYPT: Lightweight Cryptography Technique for Securing Smart Objects in Internet of Things Environment," CSI Communications, 2013.

[12] J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, "A lightweight authentication protocol for internet of things," in Next-Generation Electronics (ISNE),2014 International Symposium on, 2014, pp. 1-2.

[13] Z Bohan, W. Xu, Z. Kaili, and Z. Xueyuan, "Encryption Node Design in Internet of Things Based on Fingerprint

Features and CC2530," in Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, 2013, pp. 1454- 1457.Second Generation System-on-Chip Solution for 2.4 GHz IEEE802.15.4 / RF4CE / ZigBee. Texas Instruments. Available: http://www.ti.com/product/cc2530 (2015).

[14] A. Fragkiadakis, E. Tragos, and A. Traganitis, "Lightweight and secure encryption using channel measurements," in Wireless Communications Vehicular Technology, Information Theory and Aerospace & Electronics Systems (VITAE), 2014 4th International Conference on, 2014, pp. 1-5.

[15] L. Touati, Y. Challal, and A. Bouabdallah, "C-CP-ABE: Cooperative Ciphertext Policy Attribute-Based Encryption for the Internet of Things," in Advanced Networking Distributed Systems and Applications (INDS), 2014 International Conference on, 2014, pp. 64- 69.

[16] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things", IEEE Computer, vol. 44, pp. 51 -58, 2011.

[17] J. Brandt. (2015). 50 billion connected IoT devices by 2020. Available: http://www.smartgridnews.com/story/50-billion-connected-iot-devices- 2020/2015-04-21.

[18] T. Bradley, "Experts pick the top 5 security threats for 2015 | PCWorld," 2015-01-14 2015.

[19] M. J. Covington and R. Corscadden, "Threat implications of the internet of things," in Cyber Conflict (CyCon), 2013 5th International Conference on, 2013, pp. 1-12.

[20] S. Katzenbeisser and F. Petitcolas, "I and digital watermarking": Artech house, Boston, London 2000.

[21] N. Provos and P. Honey man, "Hide and seek: An introduction to steganography," Security & Privacy, IEEE, vol. 1, pp. 32-44, 2003.

[22] N. Tiwari and D. M. Shandilya, "Evaluation of Various LSB based Methods of Image Steganography on GIF File Format," International Journal of Computer Applications (0975–8887), 2010, pp. 35-41.

[23] D. R. Stinson, "Cryptography: theory and practice": CRC press, 2005.

[24] T. Bhattasali, "LICRYPT: Lightweight Cryptography Technique for Securing Smart Objects in Internet of Things Environment ," CSI Communications, 2013.

[25] J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, "A lightweight authentication protocol for internet of things," in Next-Generation Electronics (ISNE), 2014 international Symposium on, 2014, pp. 1-2.

[26] Z. Bohan, W. Xu, Z. Kaili, and Z. Xueyuan, "Encryption Node Design in Internet of Things Based on Fingerprint Features and CC2530," in Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conferenceon and IEEE Cyber, Physical and Social Computing, 2013, pp. 1454- 1457.

[27] Second Generation System-on-Chip Solution for 2.4 GHz IEEE 802.15.4 / RF4CE / ZigBee. Texas Instruments.Available: http://www.ti.com/product/cc2530 (2015).

[28] A. Fragkiadakis, E. Tragos, and A. Traganitis, "Lightweight and secure encryption using channel measurements," in Wireless Communications Vehicular

Technology, Information Theory and Aerospace & Electronics Systems (VITAE), 2014 4th International Conference on, 2014, pp. 1-5.

[29] L. Touati, Y. Challal, and A. Bouabdallah, "C-CP-ABE: Cooperative Ciphertext Policy Attribute-Based Encryption for the Internet of Things," in Advanced Networking Distributed Systems and Applications (INDS), 2014 International Conference on, 2014, pp. 64- 69.

[30] S. Guicheng and Y. Zhen, "Application of Elliptic Curve Cryptography in Node Authentication of Internet of Things," in 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2013, pp. 452-455.

[31] R. Watro, D. Kong, S.-f. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "TinyPK: securing sensor networks with public key technology," in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, 2004, pp. 59-64.

[32] A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, S. Mathur, and "Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks," in Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, 2013, pp. 1-7.

[33] B. Lakshmi and B. V. Raju, "FPGA Implementation of Lifting DWT based LSB Steganography using Micro Blaze Processor," International Journal of Computer Trends and Technology (IJCTT), vol. 6, pp. 6-14, 2013.

[34] M. N. B. NAIK and M. A. N. NAIK, "Steganographic Secure Data Communication using ZIGBEE", International Journal of Research in Science and Technology, (IJRST) 2015, Vol. No. 5, Issue No. II, Apr-Jun, ISSN: 2249-0604.

[35] M. S. Shahreza, "An improved method for steganography on mobile phone," WSEAS (World Scientific and Engineering Academy and Society Transactions on Systems, vol. 4, pp. 955-957, 2005.

[36] M. Shirali-Shahreza, "Steganography in MMS," in Multitopic Conference, 2007. INMIC 2007. IEEE International, 2007, pp. 1-4.

[37] D. Stanescu, V. Stangaciu, I. Ghergulescu, and M. Stratulat, "Steganography on embedded devices," in Applied Computational Intelligence and Informatics, 2009. SACI'09. 5th International Symposium on, 2009, pp. 313-318.

[38] S. Chakraborty and D. Das, "An overview of face liveness detection," International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014.

[39] "Cryptography and Network Security "by William Stallings.

[40] C.-K. Chan and L.-M. Cheng, "Hiding data in images by simple LSB substitution," Pattern recognition, vol. 37, pp. 469-474, 2004.

[41] S. A. Laskar and K. Hema Chandran, "High-Capacity data hiding using LSB Steganography and Encryption," International Journal of Database Management Systems (IJDMS) Vol, vol. 4, 2012, pp. 57 – 68.

[42] T. Morkel, J. H. Eloff, and M. S. Olivier, "An overview of image steganography," in ISSA, 2005, pp. 1-11.