International Journal of Internet of Things and Big Data
Vol.4, No.1 (2019), pp.1-8
http://dx.doi.org/10.21742/ijitbd.2019.4.1.01

National Cyber Safety and Security: Healthcare using IoT

Anitha Patil

Pillai HOC College of Engg and Tech, Rasayani, India
anithap72594@gmail.com

Abstract

Internet of Things (IoT) integration with different domains provides strategic benefits to organizations and people at large. However, when it comes to security, it is linked with national cyber safety and security in one way or other. The rationale behind this is that IoT combines physical and digital worlds and the whole digital infrastructure may be linked with IoT. Thus, it is important to leverage IoT integrations to have cyber safety and security. In this paper we considered healthcare unit as case study for IoT integration and security verification. We proposed a methodology with underlying mechanisms for searching and data sharing with end to end security. We built a prototype application realized with Things Board IoT platform and Jelastic cloud platform integrated with healthcare infrastructure. Our empirical results revealed that the proposed methodology is able to provide secure data sharing and searching in such distributed environment.

Keywords: *Internet of things, Cyber attacks, National cyber safety, Security, Secure data sharing, Cryptography*

1. Introduction

This paper is about leveraging IoT for national cyber safety and security. Internet of Things (IoT) is the amalgamation of many technologies used to have effective integration between physical and digital worlds. This is the ultimate technology that will have high impact on humans living in planet earth. Since IoT can help physical objects of any kind, including human body, to participate in computing. It helps in dramatic changes in functioning of various systems in the real world. For instance, in healthcare it is possible to have real time monitoring of patients and giving treatment to save time, effort and cost. Its intrusion into cyberspace has changed cyber security landscape. The term cyberspace has broad spectrum of meaning. It includes not only Internet and its connected devices but also hardware, software, information systems, and people involved in the interactions. Cybercrime is the crime that occurs over cyber space which is generally done by individuals or state of organization sponsored events. On the other hand cyber war is essentially a state sponsored event in large scale to defeat a nation by attacking its national critical digital infrastructure. There are three dimensions to National Cyber Security (NCS) strategy. They include governmental, the national and the international [1].

In the wake of emergence of IoT and its security and other implications, this paper proposes a methodology for investigation into IoT and national cyber safety and security. Especially, it is a new paradigm to have IoT to leverage national cyber safety and security. A nation is taken

Article history:
Received (June 16, 2019), Review Result (July 28, 2019), Accepted (September 11, 2019)

Print ISSN: 2207-3507, eISSN: 2207-3515 IJITBD
Copyright ⓒ 2019 GV Press

care of by a government. Therefore, government with respect to national cyber safety and security needs to have innovative means of protecting its digital infrastructure from cyber attacks and cyber warfare. As IoT became a reality, it is essential to leverage it to have secure cyberspace that can withstand attacks. Therefore, this paper throws light into security foundations for IoT with respect to hardware, software and information systems. Trustworthiness of elements of IoT must be rated to have trusted communications and analytics. In addition to this interoperability needs to be standardized and fostered besides accelerating leadership pertaining to IoT security.

Towards this end, this paper proposes a methodology that helps in achieving the improvements in IoT for leveraging national cyber safety and security. A case study related to healthcare domain is used for empirical study. Our contributions in this paper include the proposal and implementation of mechanisms for secure data searching and data sharing operations in IoT integrated with healthcare domain. The remainder of the paper is structured as follows. Section 2 present prior works on the IoT integration and national cyber safety and security. Section 3 presents proposed methodology. Section 4 presents the experimental results while section 5 provides conclusions and future scope of the research.

2. Related work

National cyber safety and security is an inevitable concern and challenging problem. It needs diversified approaches to protect nation from cyber attacks and cyber wars. Different approaches found in the literature including the Internet of Things (IoT) are reviewed in this section. Pfleeger and Caputo [2] emphasized the need for leveraging behavioural science so as to influence people for mitigating cyber security risk. With their qualitative research, they found the effectiveness of behavioural science for cyber security. Gubbi et al. [3] explored architectural elements and the vision of IoT for its impact on the technological world. Ubiquitous computing, common operating picture (COP), Radio Frequency Identification (RFID), Near Field Communication (NFC), 4G, 5G technologies and sensors are playing vital role in realizing IoT. IoT can be used for leveraging smart homes, transportation, community, national duties, industries, policy making, governments, individuals, and healthcare units to mention few. The vision is to combine physical things with digital things to form an integrated network for real time decision making, monitoring and so on.

Sicari et al. [4] opined that the connected devices in IoT can cause privacy, security, and trust concerns. There are different standards and communication protocols involved in IoT. The traditional security measures are not sufficient. The security challenge thrown by IoT include authentication, access control, privacy, policy enforcement, trust, mobile security, secure middleware, and confidentiality. Many European projects are working towards IoT security. They include Butler, EBBITS, Hydra, uTRUSTit, iCore, HACMS, NSF, FIRE, and EUJapan. They opined that customized security and privacy levels are to be guaranteed for IoT. Zheng and Carter [5] threw light on leveraging IoT for more efficient and effective military strategies. They opined that modern warfare can be revolutionized by leveraging IoT technologies. In military IoT can help leverage effectiveness of condition-based maintenance, real-time fleet management, inventory management, and base management and energy efficiency. Yu et al. [6] explored Cyber-Physical Systems (CPSs) in terms of the challenges and contributions of CPS for smart grids. They also emphasized the need for cyber security in the context of CPSs. Similar kind of work is carried out in [7].

Leo et al. [8] studied a federated architecture for preventing cyber attacks. The federated architecture involves multiple parties and exchange data in real time for effective disaster

response. Against cyber attacks, the architecture has mechanisms for countermeasures, isolation, diagnosis, detection, and dynamic prevention. Benson et al. [9] proposed a framework known as Safe Community Awareness and Alerting Network (SCALE) which is a CPS leveraging IoT for smart homes with potential benefits and safe communications. Benzel [10] proposed an infrastructure which reflects the science of cyber security as part of the DETER project. It has federated security mechanisms and new sharing mechanisms. Covington and Carskadden [11] specified that more objects are connected to Internet than people and the trend is growing faster with IoT technology. They analyzed security implications of IoT. They found that with IoT in place threat implications are more. Farwell [12] investigated the need for improving technologies in the wake of IoT for national cyber security. The researcher cited different security measures taken by USA government such as cyber security act, secure IT act, legal obstacles for cyber security, antitrust regulation, privacy and confidentiality, robust public-private relationships, and joint planning.

According to Ruggieri and Nikookar [13], the enabling technologies for IoT belong to categories privacy, security, future Internet, knowledge aggregation, standards, sensor networks, communication, cloud computing, discovery services, nano electronics, embedded systems, software and system integration. With these technologies IoT can be used to achieve smart cities, smart transport, smart buildings, smart energy, smart living and smart health. IoT challenges to realize such things are related to service, computation, communication, and sensors. The opportunities bestowed by IoT are low-power wireless sensors, better connectivity, zero-touch analysis, and smart services rendered to people [14]. Security issues in IoT identified in [15] include data confidentiality, privacy, and trust. Simmon et al. [16] proposed a vision pertaining to cyber-physical cloud computing for more efficient use of resources, modular composition, scalability, reliability, resiliency, and smart adaptation. Peppet [17] opined the need for making new regulations for IoT as the sensor devices associated with IoT can reveal sensitive information to third parties.

In [18], 20 security considerations are identified when cloud-supported IoT. They include secure communications, access control mechanisms, sensitive data identification, architectures, data protection in cloud, cloud data sharing, encryption by things, data combination, identifying things, identifying the provider, increase in load, logging at large scale, protecting malicious things, certification, trustworthiness, compliance audits, composite service responsibility, data location regulations, and cloud decentralization on security. Cyber security for people and organizations is explored in [19] in the context of IoT. Out of all the articles, the researchers of [5] proposed a mechanism to leverage IoT for more efficient and effective military operations. In this project, a methodology is proposed to leverage IoT for national cyber safety and security.

3. Methodology

From the literature review, it is understood that it is the IoT that will have high impact on people and organizations in future. It is also understood that it is not a single technology but made up of many enabling technologies. One such technology is wireless sensor networks that provide sensing capabilities and help in integration of physical things with digital devices. With IoT it is possible to have seamless integration of physical and digital world. This statement highlights the importance of leveraging IoT with required standards, protocols, OEM guidelines, hardware and software updates, cloud computing, secure M2M zones, interoperability, privacy, security and so on. It is the important research area which can influence national cyber safety and security. Cyber security breaches can be overcome with enhanced IoT technology usage.

Copyright © 2019 GV Press

There are many technologies pertaining to IoT especially for improving communications. They include NFC, RFID EPC and sensor networks.

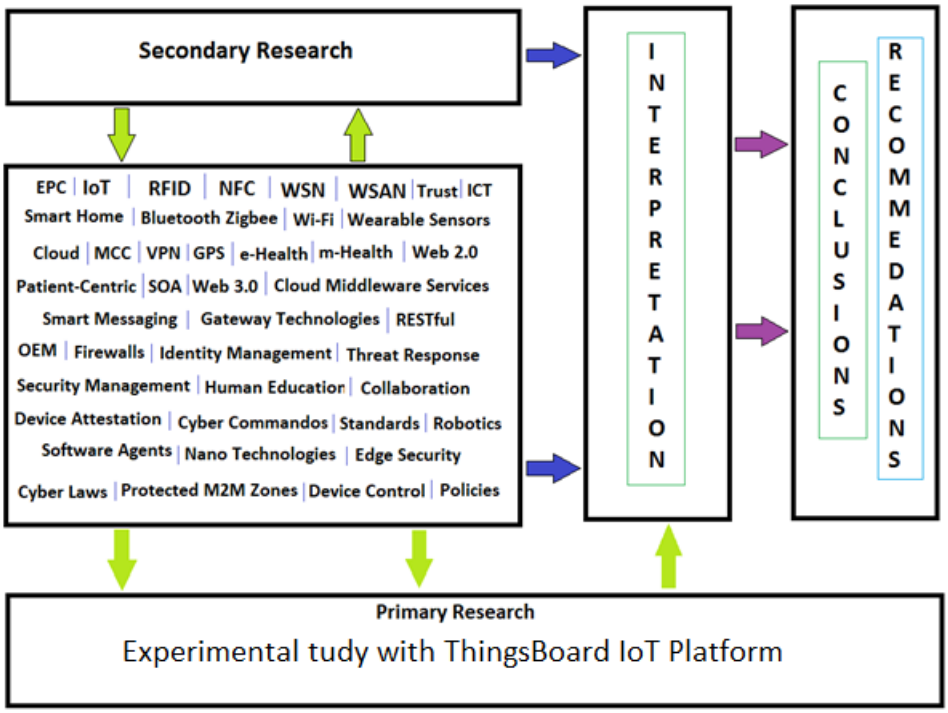

Figure 1. Proposed conceptual framework and methodology for leveraging IoT for NCS

As can be seen in [Figure 1], it is evident that secondary research is required to understand the present state of the art in IoT and its integration with different information systems. There are many things at which literature needs to be reviewed so as to get a comprehensive understanding or insights that pave way for better improvements in IoT. The secondary research is made on IoT enabling technologies and other things that are either directly or indirectly linked to IoT. EPC, RFID and NFC help in unique identification and efficient communication. WSAN is the sensor and actuator network that is widely used in IoT implementations. Existing ICT needs to be revised. The wireless technologies like Wi-Fi, Bluetooth, and Zigbee are to be views in the wake of IoT for secure and privacy preserving communications. Middleware software related to IoT programming needs to be improved to support security primitives. Wearable sensors, e-Health and m-Health architectures in healthcare domain need to be standardized. Web 2.0, Web 3.0, smart messaging and web services technologies are to be investigated for secure communications. OEMs are to be considered for improving standards in hardware and drivers. Firewalls need to be improved. Identity management plays vital role in digital world for efficient and secure transactions. Security management and threat response systems are to be studied and improved. Even when everything is secure it is possible to break a system with social engineering. Therefore, humans are to be considered part of national cyber safety and security framework. Since humans form a weak link on top of highly secure digital infrastructure, it is important to address human development and awareness issues.

4. IoT integration with healthcare unit

Healthcare is taken as case study for integration of IoT and performs secure data sharing and searching operations. The next sub section provides the security mechanisms while [Figure 2] shows a motivating scenario for the proposed work.

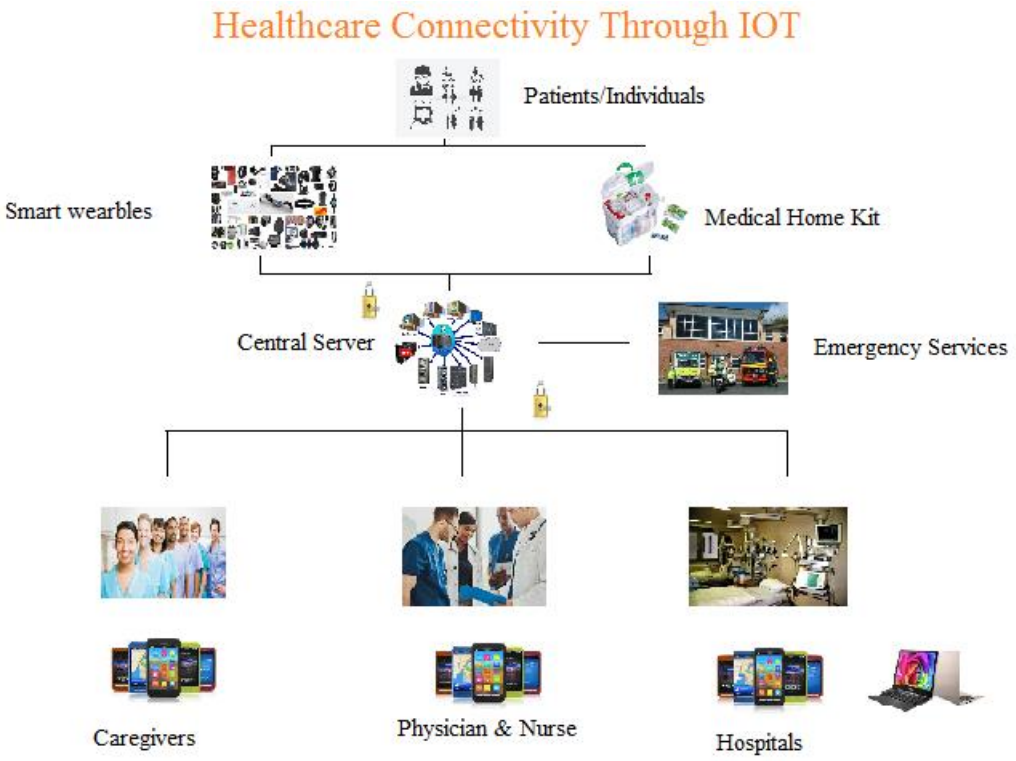

Figure 2. Motivating scenario in healthcare domain

As presented in [Figure 2], it is evident that there are many parties involved in IoT integration with healthcare unit. Smart devices, medical home kit, emergency services, care givers, physicians, nurses, hospitals etc. are connected with central server. IoT technology is used to have seamless integration. The security mechanisms are described in the subsequent section.

The user first logs in with given credentials using IoT node. IoT node generates two keys Sec key and S.Seckey. The user sends data and keywords. This data is encrypted by IOT node using these keys before uploading data to storage.

C.share ← Encrypt (Data,Sec.key)
Data can be encrypted using secret key.

C.KW.Search← Encrypt (keywords, S.Sec.key)
Keywords can be encrypted using S.sec. key.

When user logs in, his account key generation server generates public key and private key for data encryption. Secret key is encrypted by using public key. IoT node generates Dig.Cert. It gives guaranty to identify the information and also calculate hash value of data. Hash value

Copyright © 2019 GV Press

is useful when receiver checks data sent by authorized used is same or not. This hash value is encrypted by using private key.

C.Sec.Key ← Encrypt (Sec.Key, Public.Key)
H1 ← Compute hash (Data)
Signed.H1 ← Sign (H1, Private.Key)
Finally IOT Contains tuple with C.Share || C.Sec.Key || C.KW.Search || Signed.H1 ||

Dig.Cert and upload this tuple to storage under username. If authorized user wants to access the data it is login to nearest IOT node. From that storage IOT node receives tuple (*C.Share || C.Sec.Key || C.KW.Search || Signed.H1|| Dig.Cert) under username.*

IOT node check Dig Signature Then decrypt data using the following step by step procedure.

Check (Dig.Cert)
Sec.Key ← Decrypt (C.Sec.Key, Private.Key)
Data ← Decrypt (C.Share, Sec.Key)
H2 ← Calculate hash (Data)
H1 ← Decrypt (Signed.H1 , Public.Key)
Check (H1 =H2)

If hash values are matched then data sent to user authorized receiver. If matched, then data integrity is verified. This is the procedure for secure data sharing among users of the application.

Data searching and retrieval also needs end to end security. The mechanism that is employed to have secure data search and retrieval procedures.

To search some particular data on encrypted data on storage, the authorized user sends the keyword to the IOT node1 after login. The IOT node receives search keyword request secret key. Using that secret key, it generates trapdoor.

T w ← Encryption (Keyword, S.Sec.Key)

T w is sent5 to the storage with a request to search. Storage searches for the matched encrypted keywords based on the trapdoor under the username

Check (C.KW.Search, T w)

If keyword is found the corresponding tuple (C.Share || C.Sec.Key || C.KW.Search || Signed.H1 || Dig.Cert) sent to IOT. Then checks digital certificate and decrypts data step by step.

Check (Dig.Cert)
Sec.Key ← Decrypt (C.Sec.Key, Private.Key)
Data ← Decrypt (C.Share, Sec.Key)
H2 ← Calculate hash (Data)
H1 ← Decrypt (Signed.H1, Public.Key)
Check (H1 =H2)

If hash value sent by authorized user and hash value received by IOT is equal then data is sent to user. This is the mechanisms used for searching for data and retrieval of data. Thus, the proposed methodology provided end to end security in communication.

5. Conclusions and future work

In this paper, we proposed a methodology for secure data sharing and searching in IoT integration with healthcare domain. A motivating scenario of healthcare unit is considered as

case study implementation. Security mechanisms are defined and implemented for data sharing and searching with end to end security. Data download time, upload time, encryption time and decryption time are observed for different data sizes such as 10 MB, 50 MB, 100 MB and 500 MB. To have the experiments with huge data, Jelastic cloud storage is used. For IoT integration Things Board platform is used. A prototype application is built to demonstrate proof of the concept. The experimental results are evaluating by comparing our work with the prior work. The results revealed that the proposed methodology is able to provide improvements over existing work besides providing secure and efficient data sharing and searching capabilities. In future we intend to investigate on the security mechanisms that enhance the functionality of sensing devices in terms of common security attributes and standards expected.

References

[1] Mellisa E.hathway and Alexander klimburg, "National cyber security framework manual," CCDCOE, pp.1-44, **(2012)** DOI: 10.1111/j.1748-0922.2007.00176_38.x

[2] Shari Lawrence Pfleeger and Deanna D. Caputo, "Leveraging behavioral science to mitigate cyber security risk, " Computers & Security, vol.31, no.4, pp.597-611, **(2012)** DOI:10.1016/j.cose.2011.12.010

[3] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions, " Future Generation Computer Systems, vol.29, no.7, pp.1-19, **(2013)** DOI: 10.1016/j.future.2013.01.010

[4] S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol.76, pp.146-164, **(2015)** DOI: 10.1016/j.comnet.2014.11.008

[5] Denise E. Zheng and William A. Carter., "Leveraging the Internet of Things for a more efficient and effective military," CSIS, PI-IX, **(2015)**

[6] By Xinghuo Yu and Yusheng Xue, "Smart grids: A cyber–physical systems perspective," IEEE, vol.104, no.5, pp.1058-1070, **(2016)** DOI: 10.1109/JPROC.2015.2503119

[7] Pieter J. Mosterman and Justyna Zander., "Cyber-physical systems challenges: a needs analysis for collaborating embedded software systems," Softw Syst Model, Springer, vol.15, pp.5-16, **(2016)** DOI: 10.1007/s10270-015-0469-x

[8] Marco Leo, Federica Battisti, Marco Carli, and Alessandro Neri, "A federated architecture approach for Internet of Things security," IEEE, 2014 Euro Med Telco Conference (EMTC), Naples, Italy, pp.1-5, 12-15 Nov, **(2014)** DOI: 10.1109/EMTC.2014.6996632

[9] Kyle Benson, Charles Fracchia, Guoxi Wang, Qiuxi Zhu, Serene Almomen, John Cohn, Luke D'Arcy, Daniel Hoffman, Matthew Makai, Julien Stamatakis, and Nalini Venkatasubramanian, "SCALE: Safe community awareness and alerting leveraging the Internet of Things," IEEE, Communications Magazine, vol.53, no.12, pp.27-34, **(2015)** DOI: 10.1109/MCOM.2015.7355581

[10] Terry Benzel, "The science of cyber security experimentation: The DETER project," ACSAC '11 Proceedings of the 27th Annual Computer Security Applications Conference, pp.137-148, **(2011)** DOI: 10.1145/2076732.2076752

[11] Michael J. Covington and Rush Carskadden, "Threat implications of the Internet of Things," International Conference on Cyber Conflict, pp.1-12, **(2013)** DOI: 10.1109/CISTI.2015.7170475

[12] James P. Farwell, "Industry's vital role in national cyber security," Strategic Studies Quarterly, vol.6, no.4, pp.10-41, **(2012)**

[13] Ovidiu Vermesan and Peter Friess, "Internet of Things: Converging technologies for smart environments and integrated ecosystems," River Publishers, pp.1-363, **(2013)**

[14] Yen-Kuang Chen, "Challenges and opportunities of Internet of Things," IEEE, pp.383-388, **(2012)** DOI: 10.1109/ASPDAC.2012.6164978

Copyright © 2019 GV Press

[15] Shancang Li, Theo Tryfonas, and Honglei Li, "The Internet of Things: A security point of view," Internet Research, vol.26, no.2, pp.337-359, **(2016)** DOI: 10.1108/IntR-07-2014-0173

[16] Kyoung-Sook,Kim Ryong Lee ,Yohei Murakami Koji ,Zettsu,Eric, Simmon Eswaran, Subrahmanian, and Frederic de Vaulx, "A vision of cyber-physical cloud computing for smart networked systems," Nict, pp.1-61, **(2013)**

[17] Scott R. Peppet, "Regulating the Internet of Things: First steps toward managing discrimination, privacy, security, and consent," Hein online. 93, pp.85-178, **(2014)**

[18] Jatinder Singh, Thomas Pasquier, Member, I, Jean Bacon, Hajoon Ko, and David Eyers, "Twenty security considerations for cloud-supported Internet of Things," IEEE, pp.1-16, Member **(2015)** DOI: 10.1109/JIOT.2015.2460333

[19] Kenning Arlitsch and Adam Edelman, "Staying safe: Cyber security for people and organizations," Montana State University, pp.1-11, **(2014)** DOI: 10.1080/01930826.2014.893116