Virus Threat detection in IOT based Networks-New method

S.Natarajan[1]
(Research Scholar,Manonmaniam Sundaranar University,Tirunelveli,TN,India
sivnatarajan@gmail.com)
Dr.H.Abdul Rauf [2]
(Professor & Dean, Sree Sastha Institute of Engineering and Technology, Chennai, TN, India
harauf@gmail.com)
Dr.S.P.Victor [3]
(Dean of Science and Associate Professor,St.Xavier's College,Palayamkottai,TN ,Indria)

Abstract: IoT networks are growing rapidly with the fast development of wired and wireless communication technologies along with the Internet. IoT has been gradually growing in almost all important fields like education, healthcare transportation, banking and other such industries. IoT networks involve millions or perhaps billions of connected devices worldwide and perform storing as well as processing of sensitive data and information of individuals to corporate companies. The basic idea of IoT is to allow autonomous exchange of useful information between invisibly embedded but uniquely identifiable real world devices around us. IoT is fueled by the leading technologies like Radio-Frequency Identification (RFID) as well as Wireless Sensor Networks (WSNs) which are sensed by the sensor devices and further processed for decision making, on the basis of which an automated action is performed. In this paper we provide a security mechanism to identify threats in IoT based health care systems and it can also be extended to other systems. Sensor networks are particularly affected by several types of attacks. These attacks can be performed in different ways like denial of service attacks, malicious code attacks, physical attacks, and so on. To prevent threats due to viruses and other malwares in IOT systems, especially in IoT based Health care systems we suggest a new threat identification method. Our proposed method compares a file at source, destination and other required locations to identify virus threats. The experimental results are also recorded. From these results the files affected by virus threats among other files in the IoT system are identified.

.**Keywords:** IoT, RFID, Virus, Worm, Malware, Signature, Health care, Network attacks,Attack Detection Mechanism, security issues.

1 Introduction

IoT networks are growing rapidly with the fast development of wired and wireless communication technologies along with the Internet in almost all important fields like education, healthcare transportation, banking and other such industries. IoT networks involve millions or perhaps billions of connected devices worldwide and perform storing as well as processing of sensitive data of individuals to corporate companies. For example, when IoT is used in health care systems, the authorities will be able to track hundreds of patients without spending much efforts like manual systems. The term IoT was initially proposed to refer to the uniquely identifiable interoperable connected objects with radio-frequency identification (RFID) technology.

Later on, researchers relate IoT with more devices such as sensors, actuators, GPS devices, and mobile devices. Today, a commonly accepted definition for IoT is "a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'Things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network". [1]

The development of the Internet of Things [IoT] has been basically motivated by the needs of large corporations that stand to benefit greatly from the foresight and predictability afforded by the ability to follow all objects through the commodity chains in which they are connected. The ability to code and track objects has allowed companies to speed up processes, reduce errors, prevent theft and incorporate complex to flexible organizational systems through IoT. The IoT is a technological revolution that represents the future of computing and communications. The development of IoT depends on dynamic technical innovation in a number of important fields, from wireless sensors to nanotechnology [2].

The basic idea of IoT is to allow autonomous exchange of useful information between invisibly embedded different uniquely identifiable real world devices around us. IoT is fueled by the leading technologies like Radio-

Frequency Identification (RFID) as well as Wireless Sensor Networks (WSNs) which are sensed by the sensor devices and further processed for decision making, on the basis of which an automated action is performed [3].

To prevent threats due to viruses and other malwares in IOT systems, especially in IoT based Health care systems we suggest a new threat identification method. Our proposed method will identify threats efficiently to safeguard the system.

2 Literature Survey

Hui Suo et al. (2012) deeply analyzed the security architecture and features and suggested the security requirements in Internet of Things (IoT).According to them security and privacy are the key issues for IoT applications and still face some enormous challenges. In order to facilitate this emerging domain, they briefly reviewed the research progress of IoT, and pay attention to the security. They discussed the research status of key technologies including encryption mechanism, communication security and protecting sensor data.

IoT system has been facing new difficulties, severe challenges and more serious security problems. Some new technologies and methodologies should be developed to meet the higher requirements in terms of reliability, security and privacy.

Vinita Sharma et al. (2012) proposed an authentication technique in RFID for the authenticity between the tags and the reader using the technique of card generation, which has been implemented in RFID and it uses a new algorithm based on smart cards. The idea behind this algorithm in which data send through the tags can be made secure in such a way that the unauthorized users cannot access the data without any unique identification number.

Jan Henrik Ziegeldorf et al. (2013) classified and examined the privacy threats and the challenges that need to be overcome to ensure that the Internet of Things becomes a reality. Smart things allow indeed for ubiquitous data collection or tracking, but these useful features are also examples of privacy threats that are already now limiting the success of the Internet of Things vision when not implemented correctly. These threats involve new challenges such as the pervasive privacy-aware management of personal data or methods to control or avoid ubiquitous tracking and profiling. They summarized existing privacy threats into seven categories and review them in the light of the evolving IoT. Identification, tracking and profiling are long known threats which will be greatly aggravated in the IoT. The four threats of privacy-violating interactions and presentations, lifecycle transitions, inventory attacks and information linkage arise later in the IoT evolution. They represent partly new threats that have only been scratched in the related work, but can become very dangerous with regard to the predicted evolution of the IoT. The arrangement of threats in their reference model provides a clear idea of where threats appear and where to approach them conceptually. Finally, technical challenges are discussed in the context of each threat that provide clear directions for future research.

Omar Said (2013) proposed a new security model for IoT, which protect the IoT resources such as devices and data against hacking or stealing. Building IoT systems requires an accurate infrastructure planning. Furthermore, management and security of these systems are considered as the most important challenges facing system developers. Certainly, the IoT security is more than a technical problem as it needs series of regulations and faultless security system for common purposes. So, the study of IoT security problem is an emergent and the traditional techniques are studied and evaluated. The idea of proposed system is based on adaptation of the traditional algorithms to be compatible with the nature of IoT infrastructure, in addition to combining new techniques with the adapted ones to handle the research problem.

Qi Jing et al. (2014) analyzed the features and security issues of IoT, and introduced typical solutions for these issues. Also compared security issues between IoT and traditional network, and concluded that IoT system lives in a more dangerous environment with limited resources and less network guards, thus lightweight solutions would always be the first choices for IoT security. They also discussed opening security issues of IoT as an indivisible entity, and gave some potential directions for these issues.

Ashvini Balte et al. (2015) proposed various research challenges with their respective solutions. In the recent years, people need to use Internet at anytime and anywhere. Internet of Things (IOT) allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service. IOT can be distinguished by various technologies, which provide the creative services in different application domains. This implies that there are various challenges present while deploying IOT. The traditional security services are not

directly applied on IOT due to different communication stacks and various standards. So flexible security mechanisms are need to be invented, which deal with the security threats in such dynamic environment of IOT

Moeen Hassanalieragh, Alex Page et al. (2015) proposed that IoT based health networks sensors either worn on body or embedded in living environment that can help in providing rich information captured on continual basis which is aggregated and effective minded about the patient's physical and mental health. They have proposed a system where the data acquisition is performed with multiple sensors that measure physiological biomarkers.

Sapna Tyagi et al. (2016) proposed a Cloud-IoT framework to transfer medical information which represents an enabling technology for many IoT based healthcare providers to face many challenges such as rising healthcare delivery costs, information sharing, shortage of healthcare professionals, better care and enhanced services to patients. However, the benefits gained are offset by issues of trust, privacy and security in IoT based systems.

Muhammad A. Iqbal et al. (2016) concluded that traditional security primitives cannot be directly applied to IoT technologies due to the different standards and communication stacks involved. The world is undergoing a dramatic rapid transformation from isolated systems to ubiquitous Internet based- enabled 'things' capable of interacting each other and generating data that can be analyzed to extract valuable information. This highly interconnected global network structure known as Internet of Things will enrich everyone's life, increase business productivity, improve government efficiency, and the list just goes on. However, this new reality (IoT) built on the basis of Internet, contains new kind of challenges from a security and privacy perspective. To prevent unauthorized use of user's data, protect their privacy and to mitigate security and privacy threats, strong network security infrastructures are required. Peer authentication and End-to-End data protection are crucial requirements to prevent eavesdropping on sensitive data or malicious triggering of harmful actuating tasks. Any unauthorized use of data may restrict users to utilize IoT based applications.

In 2017, Sejal Patel et al. reviewed and analyzed numerous different security requirements which is used in IoT based healthcare systems. Most of the popular healthcare based research projects acknowledge the issue of the security, but they fail to embed strong security services that could preserve patient privacy. Their aim is to fulfill all the security requirements in IoT based healthcare system. In IoT based systems all sensor and devices are connected to each other so transmission and communication between those sensors become easy. In IoT based healthcare system the medical data are sensitive in nature so without considering security and privacy it is worthless. Patient medical data have to be stored in system as well as cloud, so malicious attack and unwanted access may be avoided. They also concluded that Security is most important and crucial part of IoT based healthcare systems.

3 Objective

Sensor networks are particularly affected by several types of attacks. Attacks can be performed in several ways as denial of service attacks, malicious code attacks, physical attacks, and so on.

To prevent threats due to viruses and other malwares in IOT, in particular IoT based Health care systems we suggest a new threat identification method which compares the same file at different locations and checks the code values for the file to identify virus threats. Our proposed method will identify threats efficiently to safeguard the systems from various attacks due to virus threats..

4 Importance of IoT based Healthcare Systems

In our country, providing proper medical facilities is a challenging task to the government as the population is increasing exponentially. So, it is essential to enhance the available medical facilities to the people regardless of their locations. This can be achieved in IoT based HealthCare systems. Security from various threats is an important requirement of the IoT based HealthCare systems. Different systems have various levels of security requirements. For instance, a system handling data for public usage may require low level of security than that of a patient monitoring system due to information sensitivities. Carelessness in the protection of IoT based HealthCare systems from virus and other threats may results in loss or modification of data which may cause considerable damage starting from small health problems to loss of human lives. In rural areas of our country, there are inadequate medical facilities like doctors, nurses, technicians, hospitals, laboratories, medicines, etc. The insufficient facilities in the existing healthcare systems can provide better services and solutions to the health related problems to the citizens if each and every object in the existing systems are interconnected to form IoT based healthcare system networks.

5 Existing System

With the overall development of IOT, a variety of different wireless communication technologies and network structure are accumulating, and the communication network environment has become increasingly complex. So, the basic network security issues in the IoT based systems are becoming more complex and difficult to solve.

Different approaches like centralized security solution approaches, protocol-based extensions and optimizations, certificate-based authentication, etc. are being employed to secure End-to-End communication in IoT.

Centralized security solution approaches are considered as efficient and suitable for the resource constrained sensor networks. Here a node must be pre-configured with shared keys of all entities before deployment and the common issue is the scalability of the key management.

A delegation approach delegates the public-key-based operations to a more powerful device, such as the gateway. However, the considerable RAM and ROM requirements make the use of public-key cryptography unsuitable for a wide range of constrained devices.

A proxy-based solution delegates the heavy cryptographic operations from a resource constrained device to less constrained nodes. These approaches have assumed the sensor nodes to be trustworthy and sometimes the nodes fail to deliver its assigned share.

New security paradigm are needed for End-to-End secure key establishment protocols that are lightweight for resource-constrained sensors and secure through strong encryption and authentication. In IoT applications, conventional security primitives cannot be applied especially due to the heterogeneous nature of sensors. Peer authentication and End-to-End data protection are crucial requirements to prevent eavesdropping on sensitive data or malicious triggering of harmful actuating tasks. Any unauthorized use of data may create problems to the users to utilize IoT based applications. To prevent unauthorized use of user's data, protect their privacy and to reduce security and privacy threats, strong network security mechanisms and infrastructures are required.

6 Proposed Work

Here we suggest to implement a security mechanism in which the file from IoT based Health care system is checked for file parameters at different locations mainly at source and destinations. If these code values for a particular file at different environments are matching then we conclude that the files are not infected. Here the Patient files from various data sources are received and stored in the databases of the IoT based healthcare system only after checking the code values using our proposed method.

7 Design and Implementation

Here we proposed a method in which the code value of a file in an IoT based Health care system is initially checked at different locations. By comparing these values we can identify the presence of threats due to viruses..

Our proposed system will identify the threats in IoT based Health care systems due to intruders and other malicious code activities. The algorithm used in the proposed system is given as follows:

Step 1: Initiate
Step 2: Input the Patient file from source system.
Step 3: Calculate code values SFV and DFV for the file at source and testing systems at destination.
Step 4: Compare both the code values.
Step 5: If the code values of both files match then there is no virus and other such threats.
Step 6: Send the Patient file to the destination and also store in the IoT databases.
Step 7: Otherwise repair/delete the file at destination.
Step 8: Initiate virus scanning and cleaning activities at source and destination systems.
Step 9: Request to resend the Patient file.
Step 10: End.

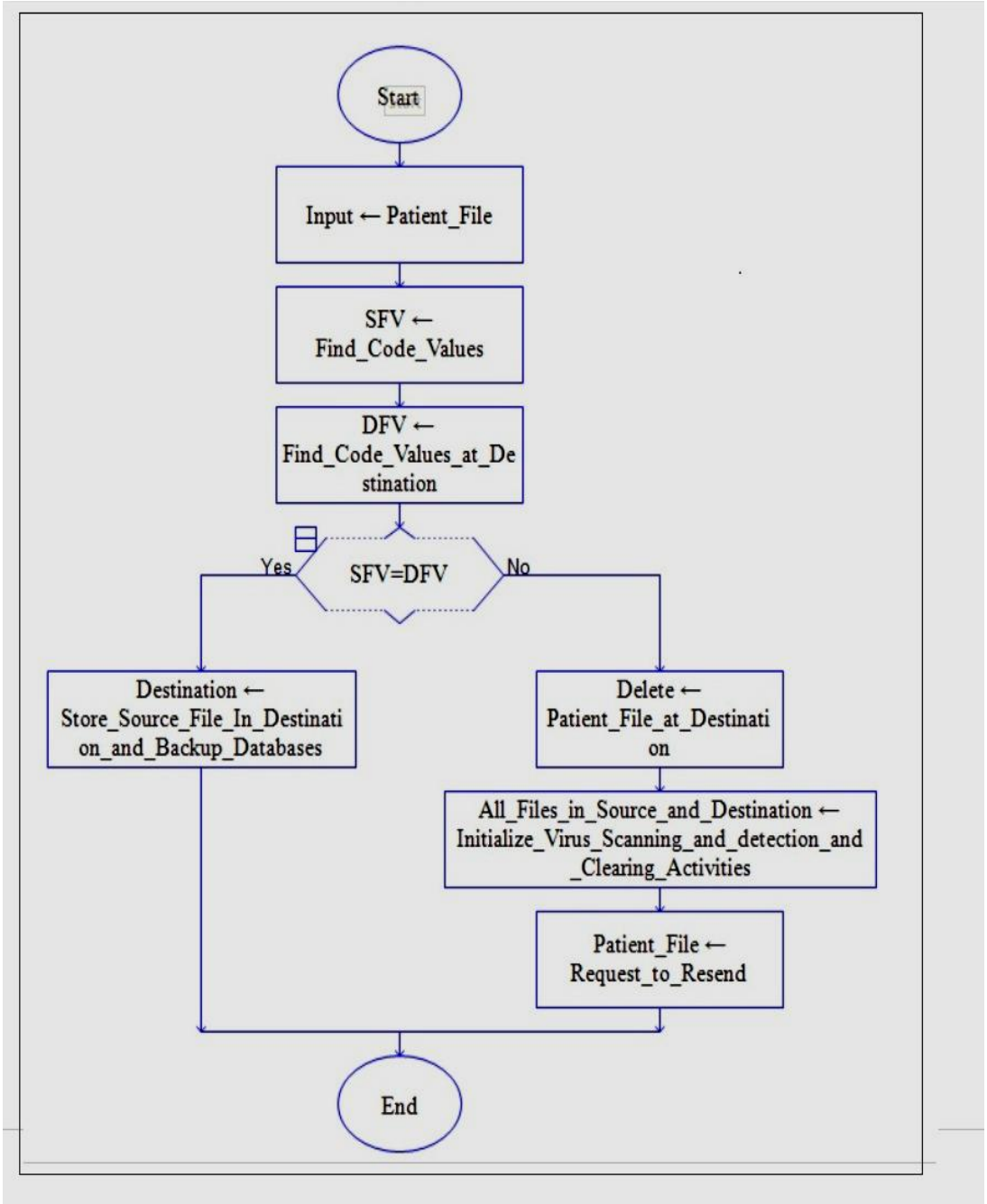

Figure 1: Flowchart of proposed Threat Identification system for IoT based health care system.

8 Experimentation and Results:

Our proposed algorithm is applied in an IoT based health care system i.e., a real-time application.

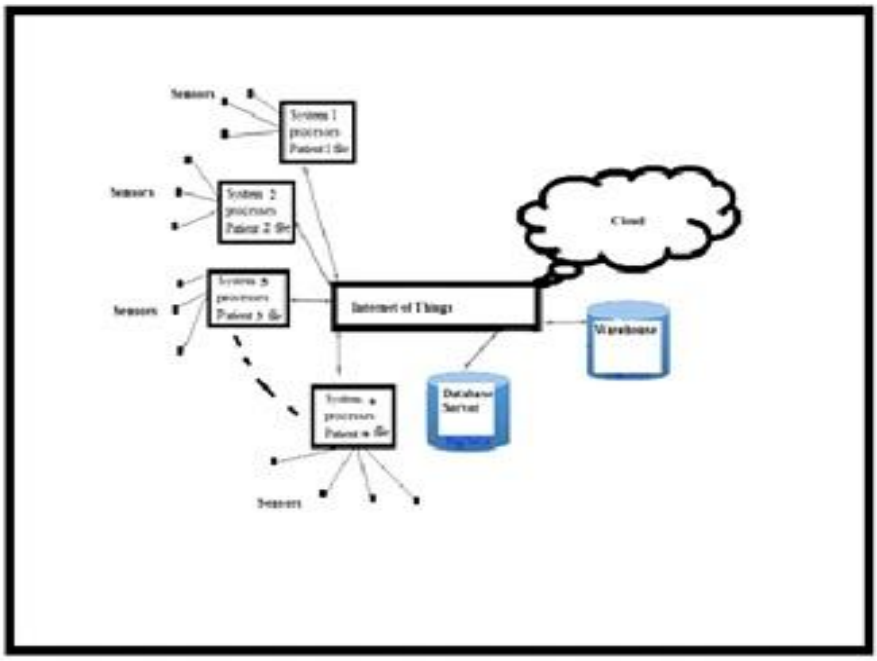

Figure 2: Block diagram of Proposed System

Here the patient files have to be sent to hospitals and doctors through the IoT based networks. By checking the code values at source and destinations we can identify the presence of threats. The results obtained using our proposed system are given in the tables:

Patient ID	Blood Pressure		Blood Sugar		Weight	Heart Beat (bpm)
	Systolic	Diastolic	Fasting	After eating		
P001	82/55	130/86	134	205	72	95
P002	77/65	102/78	102	155	62	86
P003	95/70	150/113	84	121	67	81
P004	102/81	165/120	118	175	82	105
P005	122/89	185/128	119	195	77	109

Table 1: Sample data of a patient file in the proposed system.

S. No	File name	Code values at		Result
		Source system (SFV)	Destination system (DFV)	
1	1Pranav_xray.jpg	4185D85656F2354764E84877D6CB1F13	4185D85656F2354764E84877D6CB1F13	No Threat
2	2PrilimTestsReport.docx	0784C54B0C55D81A6571F4837541EA9B	6658B3AE14EDEE22C510CF129421963A	**Threats Identified. Virus alert and Scanning initiated**
3	3Eye_Report.pdf	07EB76B66AA85E158E44AD9B95294ED8	07EB76B66AA85E158E44AD9B95294ED8	No Threat
4	4Bethel_Hospital.gif	B6BDCCD6ECD1703E4B129513F6DF03A2	B6BDCCD6ECD1703E4B129513F6DF03A2	No Threat
5	5Eye_PowerReport.jpg	66D444BB18C012DC0E196C995534A2A8	66D444BB18C012DC0E196C995534A2A8	No Threat
6	6SNHP_at_KRH_Report.bmp	887E961B45E243363141EB45573D8484	F9A4721705C5B410BDAE505E56C1FDC9	**Threats Identified. Virus alert and Scanning initiated**

Table 2: Code values for sample files in the proposed System.

In our experiments the code values are used to check the presence of threats due to viruses, malwares or other threats that changes the originality of the source files.

The following Figure 3 shows the code values during the experiment on test file 1Pranav_xray.jpg which is given at the S.No.1 in Table 2:

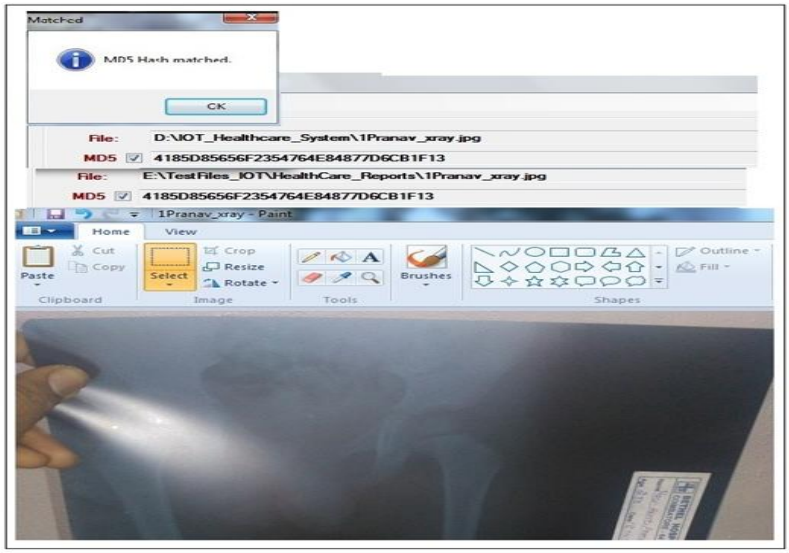

Figure 3: Experiment on test file 1Pranav_xray.jpg

The following Figure 4 shows the code values during the experiment on test file 6SNHP_at_KRH_Report.bmp which is given at the S.No.6 in Table 2:

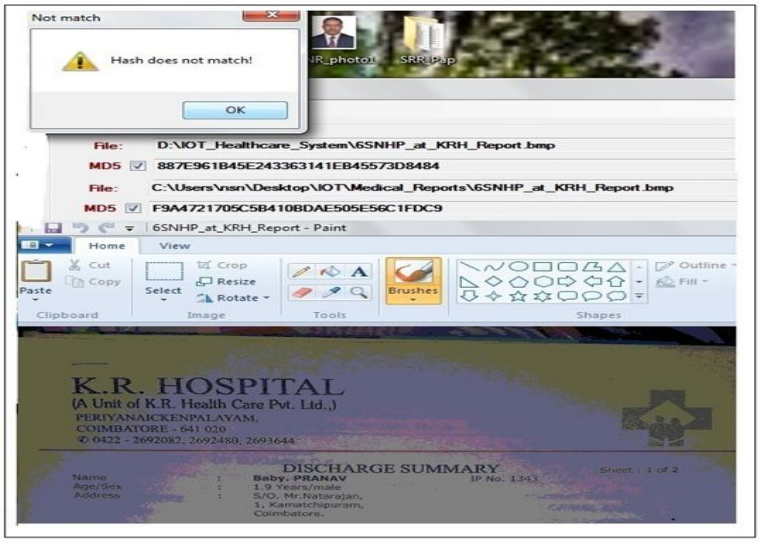

Figure 4: Experiment on test file 6SNHP_at_KRH_Report.bmp

9 Conclusion

IoT has been gradually bringing a lot of technological changes in our daily life, which in turn helps to making our life simpler and more comfortable, though various technologies and applications. IoT applications are almost in all the domains including medical, manufacturing, industrial, transportation, education, governance, mining, habitat etc. Today networks with IoT devices are having lot of threats. Viruses, other malwares and physical attacks are important causes for threats in IoT based networks components. The above threats will cause severe damages to the system. In this paper we proposed a method to overcome the above threats in IoT based health care systems. The test results are shown. The proposed method checks all the files from the IoT based health care system and filter the infected files and gives protection to the system.

10 Future Work

The above proposed method is an efficient method to store files in IoT based health care system and in their databases. This method may be considered for further research to get improvements. This method can be extended to other IOT based Systems.

11 References

[1] Internet of Things in Industries: A Survey Li Da Xu, Wu He, and Shancang Li, IEEE Transactions On Industrial Informatics, Vol. 10, No. 4, November 2014.

[2] Internet of Things (IoT): A Literature Review Somayya Madakam, R. Ramaswamy, Siddharth Tripathi Journal of Computer and Communications, 2015.

[3] A Review on Internet of Things (IoT)- M.U. Farooq, Muhammad Waseem, Sadia Mazhar,et.al, International Journal of Computer Applications (0975 8887) Volume 113 - No. 1, March 2015.

[4] Conceptual Framework for IoT-based Healthcare System using Cloud Computing , (2016), Sapna Tyagi, Amit Agarwal and Piyush Maheshwari 6th International Conference-Cloud System and Big Data Engineering (Confluence).

[5] Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-based Processing: Opportunities and Challenges,(2015),Moeen Hassanalieragh, Alex Page, Tolga Soyata, Gaurav Sharma, Mehmet Aktas, Gonzalo MateosBurak Kantarci and Silvana Andreescu, IEEE International Conference on Services Computing

[6] Security Issues in Internet of Things (IoT): A Survey, ,(2015), Ashvini Balte,, Asmita Kashid and Balaji Patil, International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 4, ISSN: 2277 128X.

[7] Development of an Innovative Internet of Things Security System, (2013), Omar said, International Journal of Computer Science Issues, Vol. 10, Issue 6,No2,ISSN (Print): 1694-0814,ISSN (Online): 1694-0784,www.IJCSI.org.

[8] Security of the Internet of Things: perspectives and challenges, (2014),Qi Jing , Athanasios V. Vasilakos , Jiafu Wan ,Jingwei Lu and Dechao Qiu, Springer Science+Business Media New York. [9] Dale R. Thompson, Jia Di, Harshitha Sunkara, and Craig Thompson, "Categorizing RFID Privacy Threats with STRIDE".

[10] Internet of Things: Features, Challenges, and Vulnerabilities-Ebraheim Alsaadi, Abdallah Tubaishat-International Journal of Advanced Computer Science and Information Technology (IJACSIT) Vol. 4, No. 1, 2015, Page: 1-13, ISSN: 2296-1739 © Helvetic Editions LTD, Switzerland .

[11] Privacy in the Internet of Things: Threats and Challenges, (2013), Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle, Special Issue Paper, Security and Communication Networks, Security Comm. Networks.

[12] A Review on Internet of Things (IoT): Security and Privacy Requirements and the Solution Approaches,(2016), Muhammad A. Iqbal, Oladiran G.Olaleye & Magdy A. Bayoumi, Global Journals Inc. (USA)Online ISSN: 0975-4172 & Print ISSN: 0975-4350.

[13] IoT based Smart Hospital for Secure Healthcare System,(2017), Sejal Patel, Narendra Singh and Sharnil Pandya, International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 5 Issue: 5.

[14] Security in the Internet of Things: A Review, (2012), Hui Suo, Jiafu Wan, Caifeng Zou and Jianqi Liu, International Conference on Computer Science and Electronics Engineering.

[15] Efficient Authentication in RFID Devices Using Et Al's Algorithm, (2012), Vinita Sharma, Jitendra Kumar Gupta and K. K. Mishra Global Journal of Computer Science and Technology Network, Web & Security, Volume 12 Issue 16 Version 1.0 ,Online ISSN: 0975-4172 & Print ISSN: 0975-4350, Publisher: Global Journals Inc. (USA).