2016 International Conference on Computing, Analytics and Security Trends (CAST)
College of Engineering Pune, India. Dec 19-21, 2016

A SURVEY ON IoT APPLICATIONS, SECURITY CHALLENGES AND COUNTER MEASURES

Ankush B. Pawar
Computer Engineering
Dilkap Research Institute of Engg. and Mang. Studies Neral, India
ankushpawar1981@gmail.com

Dr.Shashikant Ghumbre
Computer Engineering
College of Engineering,Pune.
India
shashighumbre@gmail.com

***Abstract*— Internet of Things (IoT) is a recent technology that permits the users to connect anywhere, anytime, anyplace and to anyone. In this paper, the various medical services of IoT such as Ambient Assisted Living (AAL), Internet of m-health, community healthcare, indirect emergency healthcare and embedded gateway configuration are surveyed. Further, the applications of IoT in sensing the glucose level, ECG monitoring, blood pressure monitoring, wheelchair management, medication management and rehabilitation system are analyzed. The analysis results show that the use of IoT in the medical field increases the quality of life, user experience, patient outcomes and real-time disease management. The introduction of medical IoT is not without security challenges. Hence, the security threats such as confidentiality, authentication, privacy, access control, trust, and policy enforcement are analyzed. The presence of these threats affect the performance of IoT, thus, the cryptographic algorithms like Advanced Encryption Standard (AES), Data Encryption Standard (DES) and Rivest-Shamir-Adleman (RSA) are used. The investigation on these techniques proves that the RSA provides better security than the AES and DES algorithms.**

***Index Terms*—Internet of Things (IoT), medical services, medical applications, security threats, Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest-Shamir-Adleman (RSA).**

I. INTRODUCTION

Internet of Things (IoT) has gained popularity in the recent days for interconnecting the things such as devices, sensors, equipment, software, and information services[1].It enables the communication between these things through the internet. The key elements involved in the IoT are: identification, sensing, communication, services and semantics. The identification element matches the services with the demand. The sensing element obtains the information from various objects within the network then sends back the sensed data to the cloud or to the database. The communication element interlinks the heterogeneous objects for providing the specific smart services. The computation elements are the processing units of the IoT. The microprocessor and microcontroller are some of the commonly used computation elements. The service element is classified into four classes such as information aggregation service, ubiquitous services, collaborative services and identity-related services. The final semantic element is used for extracting the knowledge from multiple machines.

According to [2], there are number of applications of IoT. In this paper, the medical applications are considered. This paper is mainly focuses on the analysis of various services and applications of IoT.

This paper is organized as follows; section II illustrates the existing IoT services and applications. Section III provides a detailed overview of the security challenges of the IoT. Section IV describes the cryptographic algorithms and anonymization techniques used for addressing the security challenges. Section V describes the results and descriptions. Section VI illustrates the proposed work and the paper is concluded in section VII.

II. MEDICAL APPLICATIONS AND SERVICES OF IOT

The IoT is used in medical sector for enhancing the quality of life, patient outcomes, management of real-time diseases and enhancing the user experience. As depicted in Fig.1, the survey on the medical applications of IoT is classified into two categories such as services and applications[5].

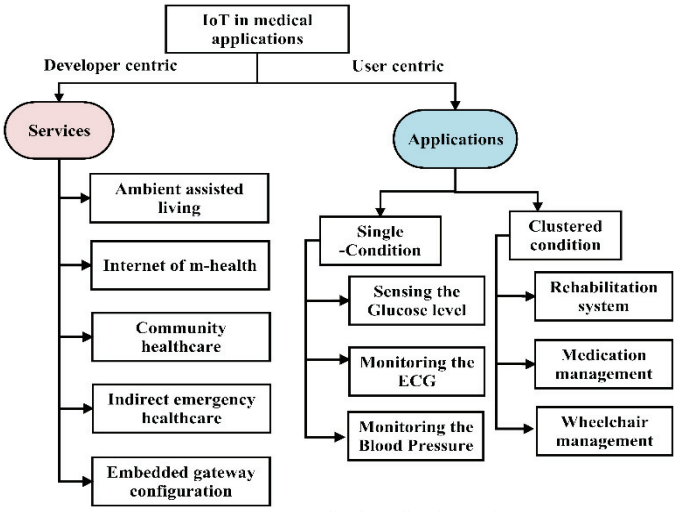

Fig. 1. Medical applications of IoT

A. Services

The popularly used IoT services are represented in Fig.1.

a. Ambient Assisted Living (AAL)

The AAL provides medical assistance for the independent living of the elderly people, disabled people, and their families. Further, it tries to provide a human-servant like assistance for any problem. In [6], an IoT-based AAL architecture is proposed for managing the blood glucose level and insulin therapy. The suggested approach monitor the patients at their home and provide a personal health card based on the RFID and web diabetes management portal. A combination of closed loop healthcare services and KIT

technology is suggested in [7] for providing a secure communication between the people and things, things and things and people and people.

b. Internet of m-health

By exploiting the medical sensors and communication technologies, the m-health provides the healthcare services. In [8], the m-IoT is used for sensing the non-invasive blood glucose level and manage them in the heterogeneous environment. The concept of 4G health is proposed in [9] for addressing the challenges in m-health.

c. Community healthcare

Monitoring the community healthcare creates an IoT network around a local community such as residential area, hospital, and rural community. The integration of multiple smaller IoT network creates a cooperative network structure. In [10], the Community Medical Network (CMN) is suggested for monitoring the medicine and health systems. The suggested CMN minimized the cost and time requirements for diagnosing and treating the diseases. With respect to the Medical and health information technology, the electronic health records of the residents are monitored in[11].

d. Indirect emergency healthcare

In [12], an immune theory-based health monitoring and risk evaluation model is proposed for monitoring the health and analyze the risks in the eastern sites. It provides highly accurate results on the health risks of the single environmental factor of earthen sites. An Intelligent Community Security System (ICSS) is proposed in [13].

e. Embedded Gateway Configuration (EGC)

The EGC is an architectural service that connects the network to the internet and other medical devices. In[14], the embedded services are exploited for the healthcare systems. An open, secure, and flexible IoT-based platform is suggested in[15] for the medical applications.

B. Applications

The applications of the IoT are classified into two types such as single condition and clustered condition. The following sections provide a short description on each of the applications.

i. Single condition

The single condition applications are meant for a particular disease.

a. Sensing the Glucose level

Diabetes or diabetes mellitus is a medical condition in which the person has higher glucose levels for a longer period.In [16], a context-aware Interactive mobile-Health System (ImHS) is suggested for providing a two-way communication between diabetic patients and IoT technology.

b. *Monitoring the ECG*

The Electrocardiography (ECG) is used for analyzing the electrical activity of the heart. In IoT based ECG monitoring, the sensors placed in the position depicted in Fig.5provides constant information about the heart rate and the rhythm. In [17], an intelligent home-based platform is proposed for improving the connectivity and interchangeability. The wearable bio-medical sensor device is connected to the inkjet printing technology.

b. Monitoring the blood pressure

Blood pressure indicates the force that the heart uses for pumping the blood around the body. In[19], a cooperative IoT approach is suggested for monitoring and controlling the health parameters such as Blood Pressure (BP), Hemoglobin (HB), blood sugar and abnormal cellular growth. An intelligent heath service is suggested in [20] for monitoring the blood pressure, diabetes, and obesity.

ii. Clustered condition

The clustered condition applications have the ability to handle multiple diseases together.

a. Rehabilitation system

As the rehabilitation system enhances the quality of life, the IoT aims at solving the issues related to aging population and unavailability of the health experts. In [21], the Body Sensor Network (BSN) is proposed for enhancing the rehabilitation exercise. An ontology-based Automating Design Methodology (ADM) is suggested in [22] for providing a smart rehabilitation systems.

b. Medication management

The issues related to the inefficient medication process are addressed by IoT. A pervasive and preventive medication management system is suggested in[23] for addressing the issues related to the medication management.

c. Wheelchair management

A smart wheelchair is an automated wheelchair specially designed for the disabled persons. The motions of the wheelchair are monitored using a computerized system. In [24], a Wireless Body Sensor Network (WBSN) is proposed for monitoring the wireless heart rate, ECG sensors, control actuators and pressure detection.

III. SECURITY CHALLENGES OF IOT

According to [26], the security challenges of the IoT are as follows,

- Confidentiality
- Authentication
- Access control
- Privacy
- Trust
- Policy enforcement

a. Confidentiality

The confidentiality ensures that the data is readable only by the destination. There exist multiple protocols and mechanisms for providing confidentiality to the data in IoT. In [27], the Datagram Transport Layer Security (DTLS) protocol is suggested for providing a two-way authentication for the IoT. In [28], multiple key revocations and key renewal protocols based on symmetric encryption and elliptic curve cryptography are analyzed.

b. Authentication

The authentication ensures the validity of user. In [29],an inter-device authentication and session-key distribution scheme are suggested for generating the session keys.

c. Access control

The access control algorithm provides new connection when communication quality ensured already. Access control is used to protect the IoT from a man in middle, replay and denial of service attacks. In [30], the Identity Establishment and Capability-based Access Control (IECAC) protocol with Elliptical Curve Cryptography (ECC) algorithm suggested for providing the access control. Multiple authentications and access control methods discussed in [31] for the IoT.

d. *Privacy*

As IoT is exploited in various applications, the users expect to protect their personal information. According to [32], the privacy concerns in IoT are classified into following:

- Privacy in device
- Privacy during communication
- Privacy in storage
- Privacy at processing

In [33], a Continuously Anonymizing Streaming data via adaptive cLustEring (CASTLE) scheme is suggested for anonymizing the data streams and ensuring the delay constraints on the data streams.

e. Trust

One of the important foundation of IoT is trust. The trust management system proposed in [35]is used for addressing the key requirements of IoT. Based on the contexts and functions, the suggested system estimates the dynamic trust scores for all the cooperating nodes. In[36], a dynamic trust management protocol is suggested for handling the misbehaving nodes.

f. Policy enforcement

In [37], an efficient enforcement security policy is suggested for addressing the security and privacy challenges. The languages used for the policy definition in[38] combined the merits of policy enforcement and analysis languages.

IV. COUNTERMEASURES FOR IOT CHALLENGES

This section illustrates the existing countermeasures for addressing the IoT security challenges. As depicted in Fig. 2, the cryptographic algorithms and anonymization technique are the two approaches used for addressing the security challenges.

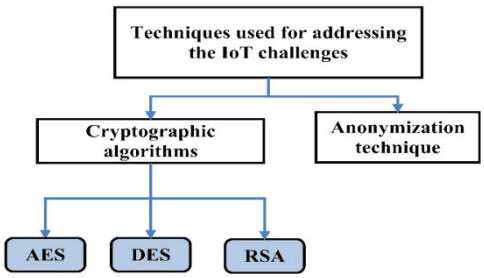

Fig.2. Categories of cryptographic algorithms

A. Cryptographic algorithms

Some cryptographic algorithms are represented in Fig. 2.

a. Advanced Encryption Standard (AES)

The AES algorithm exploits the same key for the encryption and decryption processes. The 128-bit data blocks are encrypted in 10, 12 and 14 rounds.

b. Data Encryption Standard (DES)

The DES algorithm is mainly used for protecting the unclassified data from being attacked. Similar to AES algorithm, the DES algorithm also uses the same key for the encryption and decryption processes.

c. Rivest-Shamir-Adleman (RSA)

The RSA is a public key cryptosystem that uses one public key and one private key. Among the two keys, the public key is shared with every one whereas the private key is maintained in secrecy. The RSA algorithm includes three main processes as follows,

- Key generation
- Encryption
- Decryption

i. Key generation

This step creates both the private key and public key. The overall steps involved in the key generation process are illustrated as follows[39],

Step 1: Assume two prime numbers such as *n* and *r*

Step 2: Estimate *s=nr* and $\varphi = (n-1)(r-1)$

Step 3: Choose *c* such that $1 < c < \varphi$

Step 4: Estimate the integer *i* such that $1 < i < \varphi$ where $ci \equiv \varphi$

Step 5: Return public key *(s, c)* and private key *i*

ii. Encryption

After the key generation, the plain text is converted into cipher text using the encryption process. With the generated public key, the message is encrypted by following equation,

$$C_j = m^c mod\ s \quad (1)$$

iii. Decryption

The decryption process is used for converting the cipher text to the plain text. It is based on the following equation,

$$m = C_j^i mod\ s \quad (2)$$

When compared to AES and DES algorithms, the RSA algorithm prevents multiple attacks, faster and maintains the data with more security.

B. Anonymization technique

The anonymization techniques are used for preserving the privacy of the data. For the statistical reasons, multiple hospitals reveal the details about the individuals but the presence of data in the quasi-identifying attributes, simply quasi-identifiers (QID) provide chances for the attackers to include the external information[40]. Thus, to enhance the privacy of the information, the personal data are anonymized. In [41], a privacy-preserving data publishing approach is suggested for maintaining the privacy of the individual users and preventing the sensitive information from attackers.

V. RESULTS AND DISCUSSIONS

This section illustrates the existing medical applications, security issues of IoT and the countermeasures used for addressing the limitations of the IoT. The analysis results represented in Table 1 shows that the IoT is suitable for the medical field. The existing techniques like DTLS protocol, IEAC-ECC, TMS, and CASTLE are used for the addressing the security threats. To address these security attacks, the cryptographic algorithms such as AES, DES, and RSA algorithms are popularly used. The analysis of these

techniques proves that the AES and DES algorithms are symmetric whereas the RSA is asymmetric. Further, the AES and DES algorithms are vulnerable to the brute-force attack and differential cryptanalysis attack. In addition to the cryptographic techniques, the anonymization techniques are also used for preserving the privacy of the data.

TABLE 1. COMPARISON OF VARIOUS MEDICAL APPLICATIONS, SECURITY ISSUES IN IOT AND COUNTERMEASURES USED FOR ADDRESSING THE SECURITY THREATS OF IOT

Medical applications of IoT			
APPLICATION	AUTHOR AND REFERENCE	PERFORMANCE	MERITS AND DEMERITS
Medical applications	Sung and Chiang [44]	An improved particle swarm optimization is proposed for enhancing the physiological multi-sensor data measurement	• Enhanced the data fusion performance • Provided timely medical care
	Moeen Hassanalieragh, et al [45]	Analyzed the challenges of IoT in health care monitoring	• Reduced the cost • Improved the health care
	Bhoomika and Muralidhara [46]	Designed an MCP6004 based pulse oximeter and DS1820B temperature sensor for monitoring the heart rate of the patients.	• The design system was not advanced. • The patient monitoring system was continuous.
Security threats in IoT			
THREAT	AUTHOR AND REFERENCE	PERFORMANCE	MERITS AND DEMERITS
Confidentiality	Kothmayr, et al [27]	The Datagram Transport Layer Security (DTLS) protocol is suggested for the IoT	• Low overhead • Increased interoperability
Authentication	Kang [29]	An inter-device authentication and session-key distribution system is suggested for providing the intelligent thing-to-thing communication	• Prevented the replay attacks, man-in-the-middle attacks. • Enhanced performance • Estimated the session key in prior.
Access control	Mahalle, et al. [30]	An Identity Establishment and Capability-based Access Control (IEAC) protocol with Elliptic Curve Cryptography (ECC) was suggested for preventing the security attacks	• Prevented the attacks such as man-in-the-middle attack, replay attack, and denial-of-service attack • Efficient for large scale devices
	Liu, et al. [31]	Surveyed the various authentication and access control methods	• Prevented the following attacks, ➢ Eavesdropping ➢ Man-in-the-middle ➢ Key control attack
Privacy	Cao, et al. [33]	Suggested a Continuously Anonymizing STreaming data via adaptive cLustEring (CASTLE) scheme for preserving the privacy	• Complies with the delay constraints • Have the ability to handle ℓ-diversity • Efficient
	YANG and FANG [34]	Analyzed the difference between discretionary access and limited access	• Prevented the privacy risks • Prevented the cloning of sensitive data
	Bao and Chen [36]	A dynamic trust management protocol was proposed for handling the misbehaving nodes	• Optimal than non-trust-based service composition
Policy enforcement	Neisse, et al. [37]	An enforcement security policy is suggested for addressing the privacy and security challenges	• Provided optimal communication between the IoT devices
Countermeasures for addressing the security threats of IoT			
AES	Wang, et al. [49]	Analyzed the performance of Attribute-Based Encryption (ABE), Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE)	• The evaluation results proved that the ABE was optimal for the IoT
	Mahajan and Sachdeva [39]	Analyzed three encryption techniques such as AES, DES, and RSA algorithms	• Symmetric algorithm • Faster encryption • Faster decryption • Provided higher security
DES	Mahajan and Sachdeva [39]	Analyzed the AES, DES, and RSA algorithms	• Symmetric algorithm • Had moderate speed for encryption

			and decryption processes • Has lower power consumption
RSA	Hussain [50]	Proposed the modified RSA algorithm for enhancing the security of RSA	• The application of K-nearest neighbor enhanced the security of the RSA algorithm • But, the obtained security level was not satisfactory.
	Mahajan and Sachdeva [39]	Surveyed the cryptographic algorithms such as AES, DES, and RSA	• Asymmetric algorithm • Had slower encryption and decryption

VI. PROPOSED WORK

The suggested system obtains the health data of patients from electronic gadgets and transfers them to the cloud database through the following operations,

- Pre-processing
- Key generation
- Data encryption
- Data transmission
- Data decryption

The transfer of monitored health data to the cloud database includes various security issues. Hence, to address this issue, an asymmetric cryptography based algorithm is proposed for the data transmission. The suggested algorithm exploits the Modified Rivest-Shamir-Adleman (MRSA) algorithm for performing the encryption and decryption. Further, the anonymous data storage prevents the theft from malicious users and reduces the storage space.

VII. CONCLUSION

This paper provides a detailed analysis of the various applications and services of IoT. The analysis results show that the major services of IoT are AAL, Internet m-health, community healthcare, indirect emergency healthcare, and embedded gateway configuration. Further, the applications of IoT are classified into two types such as single condition applications and clustered condition applications. The single condition applications such as glucose level monitoring, ECG monitoring, blood pressure monitoring are used for managing a particular disease. Whereas, the clustered condition applications such as rehabilitation system, medication management, and wheelchair management are used for managing multiple diseases. The introduction of medical IoT has various security challenges such as privacy, trust, confidentiality, authentication, access control, and policy enforcement. Thus, to handle these security challenges, the cryptographic algorithms and Anonymization techniques are used. The survey on the cryptographic algorithms like AES, DES and RSA proves that the RSA provides optimal prevention against multiple attacks, faster and maintains the data with more security. Based on the survey results, an asymmetric key cryptography based anonymous health data storage system is proposed. The suggested system obtains the health information of the human body and transfers them to the IoT devices. In the traditional systems, the monitored health data are transferred from the gadget to the cloud database. This includes multiple security challenges, such as man-in-the-middle attack and data hacking during the data transmission. Thus, to address these security challenges, an asymmetric cryptography based algorithm is suggested for encrypting the data before the transmission, then the Modified RSA (MRSA) algorithm is proposed for providing the key based encryption and decryption. The anonymous data storage prevents the data from malicious users.

REFERENCES

[1] H. H. G. Afshan Samani , Abdulmutalib Wahaishi "Privacy in Internet of Things: A Model and Protection Framework," *6th International Conference on Ambient Systems, Networks and Technologies* vol. 52, pp. 606-613, 2015.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials,* vol. 17, pp. 2347-2376, 2015.

[3] B. R. Ltd. (2014). *Towards Smart Farming Agriculture Embracing the IoT vision* Available: https://www.beechamresearch.com/files/BRL%20Smart%20Farming%20Executive%20Summary.pdf

[4] W. He, G. Yan, and L. Da Xu, "Developing vehicular data cloud services in the IoT environment," *IEEE Transactions on Industrial Informatics,* vol. 10, pp. 1587-1595, 2014.

[5] S. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: a comprehensive survey," *IEEE Access,* vol. 3, pp. 678-708, 2015.

[6] A. J. Jara, M. A. Zamora, and A. F. Skarmeta, "An internet of things---based personal device for diabetes therapy management in ambient assisted living (AAL)," *Personal and Ubiquitous Computing,* vol. 15, pp. 431-440, 2011.

[7] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The internet of things for ambient assisted living," in *2010 Seventh International Conference on Information Technology*, 2010, pp. 804-809.

[8] R. S. H. Istepanian, S. Hu, N. Y. Philip, and A. Sungoor, "The potential of Internet of m-health Things “m-IoT” for non-invasive glucose level sensing," in *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 2011, pp. 5264-5266.

[9] R. S. H. Istepanaian and Y. T. Zhang, "Guest Editorial Introduction to the Special Section: 4G Health—The Long-Term Evolution of m-Health," *IEEE Transactions on Information Technology in Biomedicine,* vol. 16, pp. 1-5, 2012.

[10] Y. Lei, L. Chungui, and T. Sen, "Community Medical Network (CMN): Architecture and implementation," in *2011 Global Mobile Congress (GMC)*, 2011, pp. 1-6.

[11] W. Wang, J. Li, L. Wang, and W. Zhao, "The internet of things for resident health information service platform research," in *IET International Conference on Communication Technology and Application (ICCTA 2011)*, 2011, pp. 631-635.

[12] Y. Xiao, X. Chen, L. wang, W. Li, B. Liu, and D. Fang, "An Immune Theory Based Health Monitoring and Risk Evaluation of Earthen Sites with Internet of Things," in *IEEE International Conference on and IEEE Cyber, Physical and Social Computing Green Computing and Communications (GreenCom)*, 2013.

[13] J. Liu and L. Yang, "Application of Internet of Things in the Community Security Management," in *Third International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN)*, 2011, pp. 314-318.

[14] M. F. A. Rasid, W. M. W. Musa, N. A. A. Kadir, A. M. Noor, F. Touati, W. Mehmood*, et al.*, "Embedded gateway services for Internet of Things applications in ubiquitous healthcare," in *2nd*

International Conference on Information and Communication Technology (ICoICT), 2014, pp. 145-148.

[15] X. M. Zhang and N. Zhang, "An Open, Secure and Flexible Platform Based on Internet of Things and Cloud Computing for Ambient Aiding Living and Telemedicine," in *International Conference on Computer and Management (CAMAN)*, 2011.

[16] S. H. Chang, R. D. Chiang, S. J. Wu, and W. T. Chang, "A Context-Aware, Interactive M-Health System for Diabetics," *IT Professional,* vol. 18, pp. 14-22, 2016.

[17] G. Yang, L. Xie, M. Mantysalo, X. Zhou, Z. Pang, L. Da Xu*, et al.*, "A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box," *IEEE Transactions on Industrial Informatics,* vol. 10

[18] M. P. R. S. Kiran, P. Rajalakshmi, K. Bharadwaj, and A. Acharyya, "Adaptive rule engine based IoT enabled remote health care data acquisition and smart transmission system," in *IEEE World Forum on Internet of Things (WF-IoT)*, 2014, pp. 253-258.

[19] V. M. Rohokale, N. R. Prasad, "A cooperative Internet of Things (IoT) for rural healthcare monitoring and control," in *2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)* 2011, pp. 1-6.

[20] B. M. L. a. J. Ouyang, "Intelligent Healthcare Service by using Collaborations between IoT Personal Health Devices," *International Journal of Bio - Science and Bio -Technology,* vol. 6.

[21] B. Tan and O. Tian, "Short paper: Using BSN for tele-health application in upper limb rehabilitation," in *IEEE World Forum on Internet of Things (WF-IoT)*, 2014, pp. 169-170.

[22] Y. J. Fan, Y. H. Yin, L. D. Xu, Y. Zeng, and F. Wu, "IoT-Based Smart Rehabilitation System," *IEEE Transactions on Industrial Informatics,* vol. 10, pp. 1568-1577, 2014.

[23] Z. Pang, J. Tian, and Q. Chen, "Intelligent packaging and intelligent medicine box for medication management towards the Internet-of-Things," in *16th International Conference on Advanced Communication Technology (ICACT)*, 2014, pp. 352-360.

[24] L. Yang, Y. Ge, W. Li, W. Rao, and W. Shen, "A home mobile healthcare system for wheelchair users," in *IEEE 18th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 2014, pp. 609-614.

[25] S. Ahmad and M. O. Tokhi, "Linear Quadratic Regulator (LQR) approach for lifting and stabilizing of two-wheeled wheelchair," in *4th International Conference On Mechatronics (ICOM)*, 2011.

[26] A. K. Ashvini Balte, Balaji Patil "Security Issues in Internet of Things (IoT): A Survey," *International Journal of Advanced Research in Computer Science and Software Engineering* vol. 5, pp. 450-455, 2015.

[27] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," *Ad Hoc Networks,* vol. 11, pp. 2710-2723, 2013.

[28] G. C. a. P. L. Ismail Mansour, "Key Management in Wireless Sensor Networks," *Journal of Sensor and Actuator Networks,* vol. 4, pp. 251-273, 2015.

[29] N. P. a. N. Kang, "Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle," *Sensors,* pp. 1-16, 2016.

[30] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity establishment and capability based access control (IECAC) scheme for Internet of Things," in *15th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 2012, pp. 187-191.

[31] J. Liu, Y. Xiao, and C. P. Chen, "Authentication and access control in the internet of things," in *32nd International Conference*

[32] D. R. P. J. Sathish Kumar, "A Survey on Internet of Things: Security and Privacy Issues " *International Journal of Computer Applications,* vol. 90, pp. 20-26, 2014.

[33] J. Cao, B. Carminati, E. Ferrari, and K. L. Tan, "CASTLE: Continuously Anonymizing Data Streams," *IEEE Transactions on Dependable and Secure Computing,* vol. 8, pp. 337-352, 2011.

[34] J.-c. YANG and B.-x. FANG, "Security model and key technologies for the Internet of things," *The Journal of China Universities of Posts and Telecommunications,* vol. 18, pp. 109-112, 2011.

[35] Y. B. Saied, "Trust management system design for the internet of things: a context-aware and multi-service approach," *Computers & Security,* vol. 39, pp. 351-365, 2013.

[36] F. Bao and I.-R. Chen, "Dynamic trust management for internet of things applications," presented at the Proceedings of the 2012 international workshop on Self-aware internet of things, San Jose, California, USA, 2012.

[37] R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the Internet of Things," in *2014 IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2014, pp. 165-172.

[38] Y. Elrakaiby, F. Cuppens, and N. Cuppens-Boulahia, "Formal enforcement and management of obligation policies," *Data & Knowledge Engineering,* vol. 71, pp. 127-147, 2012.

[39] P. Mahajan and A. Sachdeva, "A study of Encryption algorithms AES, DES and RSA for security," *Global Journal of Computer Science and Technology,* vol. 13, 2013.

[40] G. Ghinita, Y. Tao, and P. Kalnis, "On the anonymization of sparse high-dimensional data," in *IEEE 24th International Conference on Data Engineering*, 2008, pp. 715-724.

[41] W. K. Fung BCM, Chen R, Yu PS. , "Privacy-preserving data publishing: A survey of recent developments.," *ACM Comput. Surv.,* vol. 42(4), 2010.

[42] G. Baldini, M. Botterman, R. Neisse, and M. Tallacchini, "Ethical Design in the Internet of Things," *Science and Engineering Ethics,* pp. 1-21, 2016.

[43] B. Zhou, J. Pei, and W. Luk, "A brief survey on anonymization techniques for privacy preserving publishing of social network data," *ACM Sigkdd Explorations Newsletter,* vol. 10, 2008.

[44] W.-T. Sung and Y.-C. Chiang, "Improved Particle Swarm Optimization Algorithm for Android Medical Care IOT using Modified Parameters," *Journal of Medical Systems,* vol. 36, pp. 3755-3763, 2012.

[45] A. P. Moeen Hassanalieragh, Tolga Soyata, Gaurav Sharma, Mehmet Aktas, Gonzalo Mateos, Burak Kantarci, Silvana Andreescu, , "Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-based Processing: Opportunities and Challenges," *IEEE International Conference on Services Computing,* pp. 285-292, 2015.

[46] K. N. M. Bhoomika.B.K, "Secured Smart Healthcare Monitoring System Based on IoT," *International Journal on Recent and Innovation Trends in Computing and Communication* vol. 3, pp. 4958-4961, 2015.

[47] N. M. C. Meria M George, "Patient Health Monitoring System using IOT and Android," *Journal for Research,* vol. 2, pp. 102-104, 2016.

[48] G. W. S. S. S. Aruna Devi.S, "Patient Health Monitoring System (PHMS) Using IoT Devices " *International Journal of Computer Science & Engineering Technology (IJCSET),* vol. 7, pp. 68-73, 2016.

[49] X. Wang, J. Zhang, E. M. Schooler, and M. Ion, "Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT," in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 725-730.

[50] A. K. Hussain, "A Modified RSA Algorithm for Security Enhancement and Redundant Messages Elimination Using K-Nearest Neighbor Algorithm " *International Journal of Innovative Science, Engineering & Technology (IJISET),* vol. 2, pp. 159-163, 2015.