INTERNATIONAL RESEARCH JOURNAL OF SCIENCE ENGINEERING AND TECHNOLOGY



ISSN 2454-3195

An Internationally Indexed Peer Reviewed & Refereed Journal

WWW.RJSET.COM
www.isarasolutions.com

Published by iSaRa Solutions

DESIGN HEALTHCARE FRAMEWORK FOR IOT NETWORK AND SECURITY ISSUES

Harshita Vachhani[1], Dr. Jitendra Sheetlani[2], Dr. Sachin Kadam[3], Dr. Vishnu Mishra[4] Dr. Megha Mishra[5]

1 Dept. of Computer Science, Research Scholar (Ph.D), SSSUTMS University, Sehore(M.P) ,466001, India

2 Dept. of Computer Science, Professor, SSSUTMS University, Sehore(M.P) ,466001, India

3 Director -ICT, Bharati Vidyapeeth (Deemded to be University), Pune (Maharashtra) ,411030, India

4,5 Dept. of Computer Science, SSGI-FET, Bhilai, Chhattisgarh, 491001, India

Corresponding Author: **profharshita@gmail.com**

Abstract :- This paper emphasis to on evaluation of security issues, model, Challenges, suitability of IoT healthcare system. The IoT healthcare different challenge are including smart sensor computing, smart pills, different security and privacy issues, low-power operation of remote device. The Internet of Things (IoT) has many different prospective to make over healthcare by overpoweringly changing how hospitals, clinics and other concern services assemble and utilize information by bringing together the most important scientific and industry trends of mobility, automation and data analytics to develop patient care delivery. IoT basically means to connect the substantial things such as embedded sensors, actuators and additional devices that gather and broadcast communication messages concerning real-time action, via a network. The data gathered from these devices can then be analyzed by the organization. The work carried out during this research is consequently formulate a exclusive contribution in that, it recognizes all key mechanisms of an end-to-end Internet of Things healthcare organization, and recommends a generic model that could be useful to all IoT-based healthcare organizations. This is crucial because presently no recognized end-to-end structure for remote scrutinizing the physical condition in the literature. The proposed work present and solve the IoT security problem, focus different issues occur during IoT healthcare and there devices. This thesis wraps various suggestions for future research. The overall experimental results generated the utilization of the IoT device.

Keyword: - Internet of Things, healthcare, medical environments, sensors.

Introduction

There are many IoT architectures, technologies, and design methodologies intended and govern security issues. The visualization and cloud infrastructure monitor and manage IoT devices security and data, the same IoT security device use encryption and decryption algorithm. There are different layers of internet of things architecture and these layers utilize different topologies and equipment for maintain the privacy security, standardization of sensor data. There are many middle ware working between theses layers and provide coordination of each individuals parameters evolve in IoT healthcare system. The Privacy and security are diverse to each other, though in healthcare field, the association among individual's two concepts is provide protection in healthcare system. There are mutual relationship between security and privacy that is, confidentiality is located in the intersection of privacy and security that is, confidentiality is located in the. The security, privacy and protection are backbone of network security system and each and every one among are diverse. These are backbone of healthcare also and IOT healthcare system presently provide five layers these are Perception layers it also called Edge layers, Transport layers ,Processing layers Application and Business layers. In current technology, the communication is mainly oriented from devices to the end-user and the Internet is used to connect these end-user devices. The focus of IoT, on the other hand, is on the autonomous interaction of smart objects without using humans as an intermediate

station. The connected smart objects interact, collect and share data in the background, which in the end creates useful information for an end-user or influences the end user's actions.

RFID systems can help us find our lost items by checking the last recorded location. Furthermore, the user could search for keywords and if the condition matches the location the item could be found. This option of item tracking can even be used to detect theft. In case an item, that is part of a restricted area, has been removed from this area without authorization despite all of these promising innovations, the Internet of Things, as every other technology, faces multiple security challenges. Information is one of the most important assets in any stream whether its education system, organizations, healthcare, transportation etc. Information is valuable and should be appropriately protected. Security is to combine systems, operations and internal controls to ensure integrity and confidentiality of data and operation procedures. Information is one of the most important assets in any stream whether its education system, organizations, healthcare, transportation etc. Information is valuable and should be appropriately protected .Security is to combine systems, operations and internal controls to ensure integrity and confidentiality of data and operation procedures. Mainly there are five Information Security goals in an organization: Confidentiality, Integrity, Availability, Authorization and non-repudiation. On the device (object) side, we broadly have two layers. The first is the object layer, which allows a device to connect to other devices, talk to them (via standardized protocols), and exchange information. The object layer passes information to the social layer. The social layer manages the execution of users' applications, executes queries, and interacts with the application layer on the server. IoT healthcare have following layers.

i. Application layer: The application layer work as upper layer of any environment. Here various application and protocols deploy for monitoring and controlling the healthcare system.
ii. Processing layer: This layer responsible for network data mining purpose. Network data mining means it store large amount and data and analyze that data which come from Transport layer
iii. . Network layer: The network layer connects different smart devices, equipment and different servers for processing and getting information from different network and sensors.
iv. Perception layer: This layer is also known as the physical layer, this layer collect information from environment by using some physical parameters. These parameters recognize by different object and define environment.

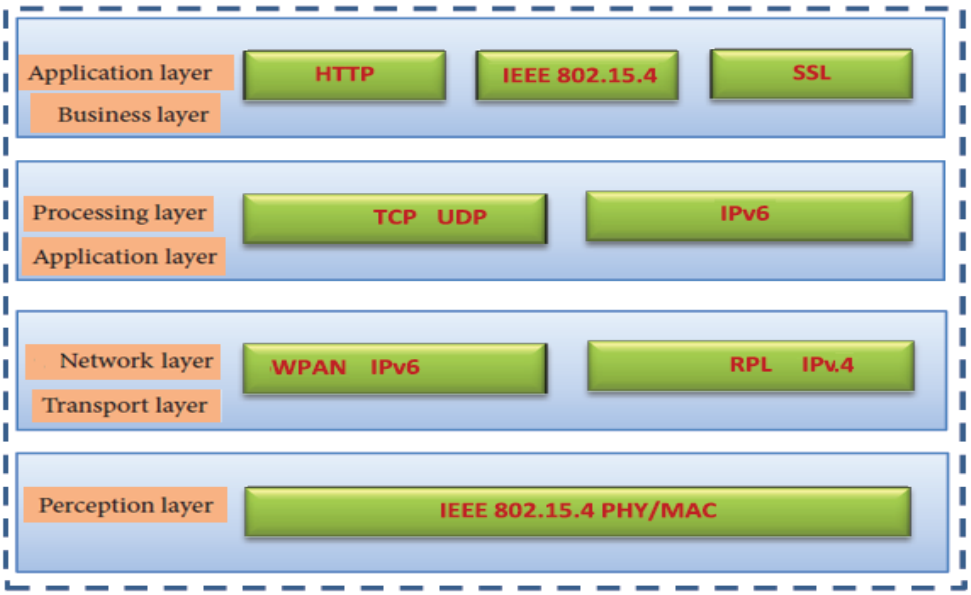


Fig:- Internet Of Things healthcare network Security model.

The recent IOT based healthcare system use five layer of protection protocol, high level security, secure algorithm/protocol, secure system architecture, short range of communication. The remote healthcare security recognizes with novel 5G IoT healthcare security system that provides more security, privacy and protection. The purpose of IoT based healthcare architecture system to increase the medicinal facilities on remote hospitals, assign smart medical agent, and solve sensitive and serious activity. RFID chip solve informality problem of medicines and diagnose system. This work moreover attempt to identify different security occurs in healthcare system an how we resolve that problems. This work describes features, services pros and cons of IoT based healthcare security system. The one main objective to describe power and usability of medical sensors and their security aspects, sensors use wireless device, sensors measures crucial patient. IoT based healthcare system provide roubust, secure, protective environment that increase the utilization of healthcare technology and society associated it. The IOT security architecture play main role to concern increase privacy of healthcare system with confidentiality. Misuse of data and information also focused on this associated exertion. The sensor holding all data and information reading healthcare and leaking of such information affected the sensitivity of healthcare care system

Information Integrity

The assessment of IoT facilitated skills for physical condition and comfort; including sensors, functioning systems, growth and processing structure, and amalgamation policy is provided in [2]. In the same way, a comprehensive outline for wireless system is specified in [3], maintaining the perception of mobile healthcare applications. They assess a wide variety of communication skills including cellular, wireless LAN and satellite connections. They recommend diverse skills that can be utilized by planning the technical facility with the functional necessities. The instigator wind up with the challenges such as network overcrowding, elevated packet thrashing and suggested to little consistency, and non-deterministic presentation with the provisos of latency, interruption, or throughput, should be attend by the forthcoming superior wireless and cellular communication broadcast equipment, including 5G. Initiated an additional policy reliant on the 5G communications organization which identifies the significance of service improvement “in multi stakeholder surroundings”. It acquires a systems’ amalgamation scheme for industry replica to provide the conversion in the technique for conveying healthcare that is convey by ICT. The suggestion is to develop flexible strategies that allow each actor to focus on its core competences; providing interfaces between different business roles [7]. This proposition is not supported by any empirical data and it is not clear how predefined business roles are compatible with innovation in the sector. However, the framework provides a common setup to develop and discuss roles and relationships; with emphasis on the technology providers. Healthcare devices can be categorized into four types:-

i. Stationary Medical Devices—devices can be used on a specific physical location (e.g., chemotherapy dispensing stations for home-based healthcare)

ii. Medical Embedded Devices—devices which can be implanted inside the body (e.g., pacemakers)

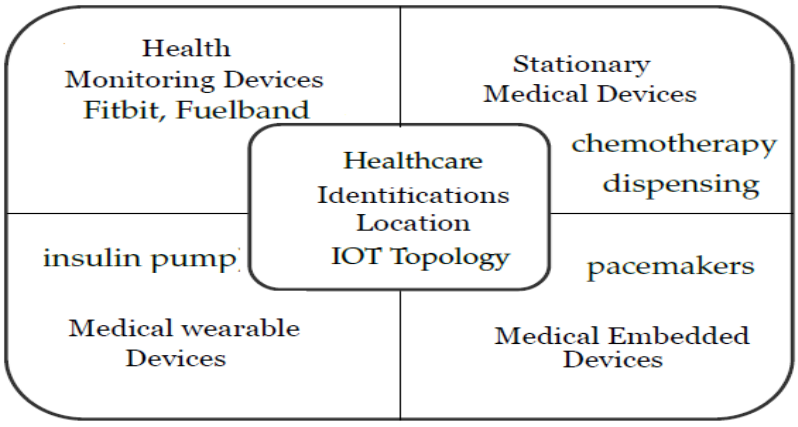


Fig:- Internet of Things security layer devices architecture.

iii. MedicalWearable Devices—prescribed devices by doctors (e.g., insulin pump)
iv. Wearable Health Monitoring Devices—consumer products (e.g., Fitbit, Fuelband, etc.)

The basic after reviewing this wide range of existing IoT-based healthcare system, several requirements for the design of such systems become apparent. Each of these papers emphasizes the use of sensors for monitoring patient health. All observed wearable sensors, namely wireless and externally-wearable sensors, as crucial to their individual systems. Numerous mechanisms [10], also recommended the use of environmental or vision-based sensors around the residence. In smart healthcare applications, IoT sensors/devices are introduced to patients in aspects. The patients' health information (data) are collected from ECG, fetal monitors, temperature, or blood glucose levels and safety of this data is crucial regarding patients' lives. Computer science and IoT community, and healthcare providers have been struggling secure each and every sensor/device in the IoT network with the integrity of its data. Though the safety and comfort of patients' everyday health relies on this data collection, the safety of the data is greatly affected by cyber threats/attacks. In addition, patients' privacy sensitive data can also be affected. A conventional explanation frequently proposes protection to patients' physical condition supervising facts throughout the communication. Though, they habitually are unsuccessful to agreement with complex assaults at the time of information change into cipher and subsequent to the cipher broadcasting. Ransom ware, DDoS attacks, insider, e-mail compromise, and fraud scams are common types of attacks in healthcare [9]. Besides, there are types of attacks that are very related to communication, including eavesdropping, impersonation, data integrity, data breach, collusion, and so on. Particularly, these threats/attacks bring new challenges, for example, data can be compromised during the data communication [1], by which patients' personal data can be revealed. Belongings (IoT) consist of mechanically and cleverly associated sensors and actuators that are incorporated in equipments and substantial things. IoT technologies lead our life to interact with the sensors/devices of the world and leverages collected smart data from them to facilitates our life so easy and convenience [1]–[5]. These technologies have now been known as an example of a smart cyber-physical systems, which also incorporate technologies of many related emerging systems, including smart energy and grids, smart power plants, smart home monitoring, smart cities, and smart healthcare system [6]–[8].

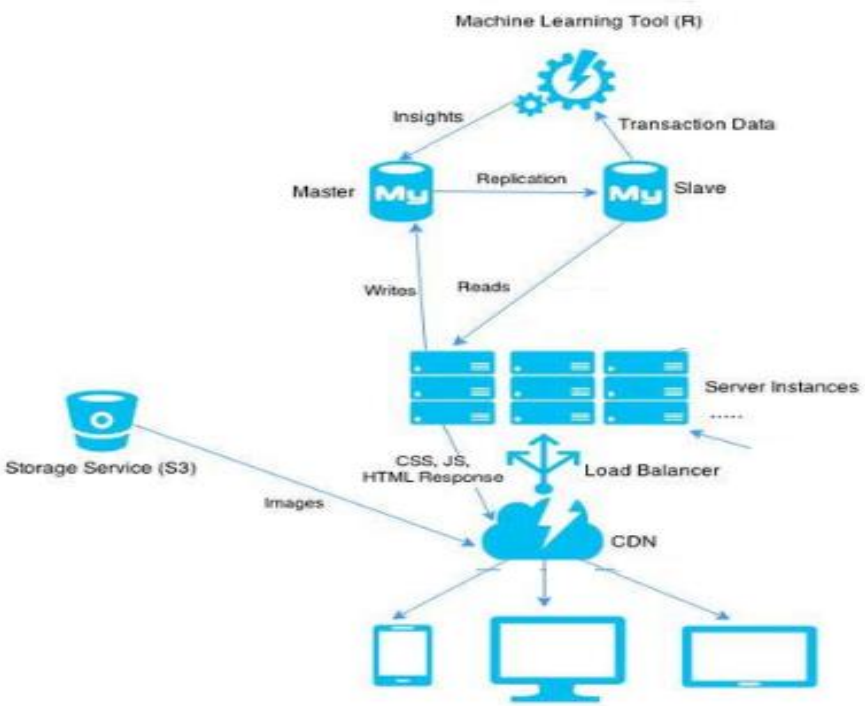


Fig: - Internet of Things cloud architecture healthcare system for security.

The cloud based architecture has following features, these are: Cloud Architecture for Health: The research has been conducted in recent years regarding the benefits of cloud for healthcare applications. These benefits stem from the three primary services that can be provided by cloud technologies in healthcare environments:

i. Software as a Service (SaaS) - provides applications to healthcare providers that will enable them to work with health data or perform other relevant tasks.
ii. Platform as a Service (PaaS) - provides tools for virtualization, networking, and database management.
iii. Infrastructure as a Service (IaaS) - provides the physical infrastructure for storage, servers, and more.

The message format of CoAP is a simplified version of HTTP. It is typically designed for the communication between resource constrained devices. Constrained environment and internet environment are bridged through proxy devices. The data flow of the IoT can be divided into four phases, data collection, data transmission, data storage, and data analysis. The figure shows the data flow format of the IoT.

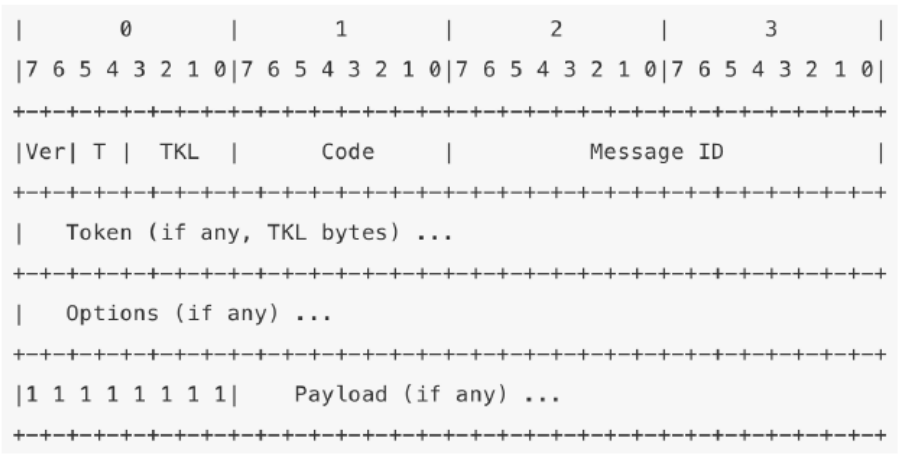


Fig: - Internet of Things Message format system for security.

The Ver" is a 2-bit unsigned integer. It mentions CoAP version number. "T" is a 2-bit unsigned integer. It indicates message types: CON (0), NON (1), ACK (2), RST (3). "TKL" is a 4-bit unsigned integer. It indicates the length of token (0-8 bytes). "Code" is an 8-bit unsigned integer. It is combined with 3-bit class representing a request (0), a successful response (2), an error response from client (4), or an error response from server (5), and 5-bit detail. The last two bytes are network byte 0 order according to big-endian order. Followed by "Token" that associates a request and a response. Then there is option or multi-options. There could be no payload after options.

Information Confidentiality

The accessing the cloud data user authentication or verification play important role for security enhancement. Therefore, third phase of cloud environment engages the security measurement and prevent unauthorized user accessing the IoT based cloud environment. That increases the utilization factor of healthcare system. Therefore this technique, produce a feature interrelated to cipher text and according to this attribute the user authentication is handled. The most important part of the projected algorithm provides and also permits the innovative appearances to decide the introduction as groups above GRQ. This helps to avoid any further collision with the existing collided requests waiting in the queue.

This security algorithm focus on encryption process for cloud encryption process is described below:

Cloud Encrption Algorithm (128-bits)

……

Step 1: Start
Step 2: Insert text data (D) and private key (128-bits) (P) by Cloud User.
Step 3: User text data (D) and key (P) reach at Cloud Server End.
Step 4: Read User text data and key (128-bits) at Cloud End.
Step 5: Apply algorithm „RSA to T.
Step 6: Produce Initial level cipher text CT1.
Step 7: Prepare Encrypted key (EK)
Step 7.1: Generate KG using algorithm „Gen.
Step 7.2: Apply algorithm „EnK to generate KG.
Step 8: Pass CT1 and KG to next level algorithm.
Step 9: Produce Second Level of cipher text CT2 by applying algorithm „PAE.
Step 10: Pass CT2 to algorithm „ABC to generate an attribute „α.
Step 10: Stop

In first phase ciphering technique has been developed which offer preliminary level security and by the side of the similar time it give more accurate key. The second stage of projected effort arrangement with new designed encryption algorithm which is based At last but not least, it is very obvious that while talking about the security of the data the cryptographic encryption technique plays an important role but similar time it is very essential to verify authentication privileges of the different user who tries to access these cloud-disk stored data.

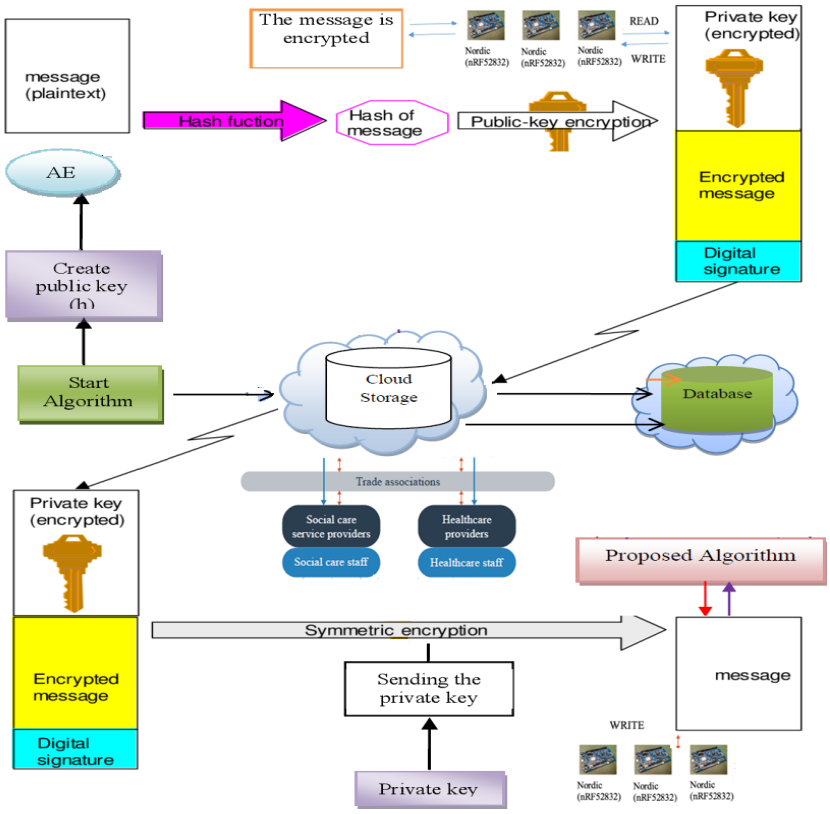


Fig: - Security Algorithm block diagram

The proposed working model for a public key technique describe the lightweight security approaches which is suitable for all electronic devices, distributed devices and mobile/portable devices constrained. The IoT based healthcare devices make use of unusual communication technologies, like Wi-Fi, 4G, WiMAX and Bluetooth technologies. This effort increase the utilization factor according to time and concern the substantiation message along with communicating devices to avoid Mit M attack. The authentication process of this work carried out in three sequential phases.

Result and Analysis

In this section, we study the relationship cryptography and security, we use Python Flask framework to form servers in both the entry point and BLE master, and Amazon server is the base of Flask. AWS is easy to parse HTTP header and payload, and it integrates routing system to match URLs. Additionally, Flask naturally supports multithreaded mode. Then, Flask is able to run concurrent Web services. The sensing data of Nordic endpoints represents virtual resources that are read by BLE master, and then the BLE master POST data as payload in JSON format to the entry point at every certain period. Finally, an end point registers in the Fog server that stores all information into database. The URL exposed by the entry point represents an API for a BLE master to access. The payload is written in JSON format as name / value pair for efficient and easy data parsing. Figure 5-1 is an example of a request from an endpoint, including a URL, a JSON-formatted payload, and an API to send a HTTP POST request.

```
url='http://192.168.0.104:9943/IoT/'

value='{" tiredness r":"%d %s","cough  ":"%d %s"}' % (T, " fever ", H, "%")

payload={'value':value, 'boardName':'nRF52832_0', 'programVersion':'v1.0.0', 'location':'MADMUC-RM178.9', 'remoteHostPath':'/nRF52/', 'mac':'D9:C7:9A:5E:43:30'}

r=requests.post(url, data=payload, timeout=sys.maxint)
```

Fig: - Request format for POST API server

The widespread utilization of virtualization for executing cloud communications conveys exclusive protection apprehension for clients or occupant of a community cloud service. Virtualization changes the association connecting the OS and fundamental hardware and be used for calculation, storage or still for networking.
This establishes a supplementary level - virtualization - so as to itself have to be appropriately configured, administer and protected. Detailed concern comprises the possibility of negotiation for virtualization of software, or "hypervisor". Although these concerns are principally hypothetical, they do survive.

Parameter	**nRF52832 System peripheral**
Number of dedicated Oscillator	64 MHz from 32 MHz external or internal crystal with RC synthesized
Security preamble retransmission(P/Sec)	128-bits AES
Wireless Protocol support /air data	Bluetooth 2.4/ 2Mbps/1 Mbps
Maximum number of Radio Frequency/ MSC range	7mA/128 bss cellular miles
Energy type	Low
Total Processor performance	144 core mark
Actual Temperature required	85 to 105

Table: - The suggested parameters for nRF52832 comparison

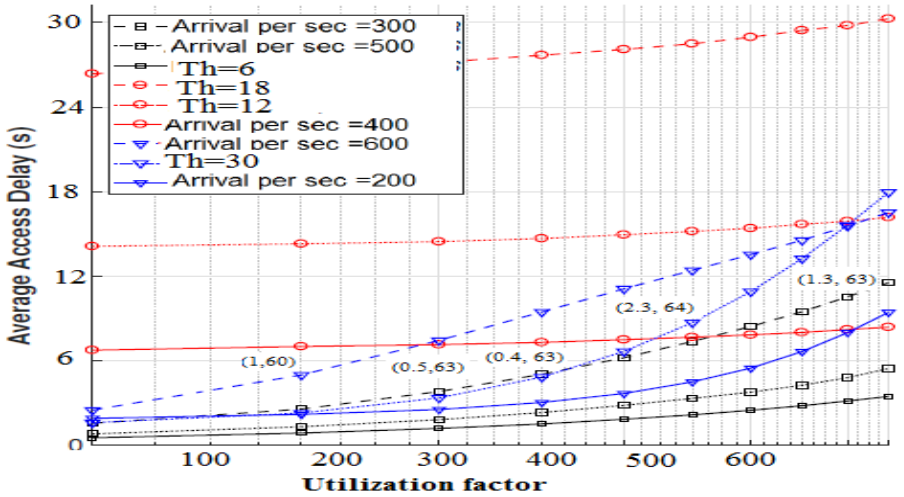
In several replicas, there are three major protection necessities that required and also addressed in the direction of replica designer: privacy, reliability, and accessibility. Privacy creates definite way that merely approved and client can access the system. Reliability is dependable for communication, sent to the objective not including any modification, and accessibility means information is forever obtainable to the client when desired. The security stability threshold effect is a most impressive property for block ciphering and hash function algorithms. The avalanche effect circumstance is fulfilled in following conditions: If the output changes considerably (e.g., half the output bits flip) causes a minor change in input (e.g., flipping a single bit). In block ciphers, such a small change in either the key or the plaintext should grounds to a strong change in the cipher text. The above conditions of avalanche effect allow small changes to propagate rapidly through iterations of the algorithm; in such a way that every bit of the output should depend on each fragment of the input message earlier to the algorithm expires.

Security stability Threshold Formula is given below: Security stability Threshold effect =Number of change bits in cipher text number of bits in cipher text

Input Utilization factor	Security stability Threshold (Th) Arrival rate	Security stability Threshold value (Th)	Virtual Group Size	Max value bits change(per second)
(1,60)	200	6	(1,6)	96
(0.5,63)	300	12	(0.5,12)	93
(0.4,63)	400	18	(0.4,18)	97
(2.3, 64)	500	24	(2.3,24)	110
(1.3,63)	600	30	(1.3,30)	98

Table**:** - The threshold effect analysis with utilization factor comparison

The experimental evolution focus on actual data Bytes or Char conditions of avalanche effect allow small changes to propagate rapidly through iterations of the algorithm; in such a way that each chunk of the output will be supposed to depend on every chunk of the input before the algorithm expires.



The overall results of above conditions of avalanche effect allow small changes to propagate rapidly through iterations of the algorithm; in such a way that every bit of the output should depend on each fragment of the input message earlier to the algorithm expires. What we want to emphasize here is that the security of per bits data requires almost perfect coordination between all parameters in accordance with a specific load to achieve the performance level similar to what ours has to decide.

Conclusion

The performance of this research work the concept of proposed technique including the various encryption schemes of system based on the various type of key and proposed encryption algorithms. The proposed technique provides a framework for confidentiality of text information in cloud storage data at cloud environment that can be useful in various applications which is required for storage of data at cloud end. Benefits to the proposed technique include the simplicity and confidentiality. The security analysis shows that the produced avalanche effect strengthens the proposed technique which is based on the "proposed algorithm". Future work can present an enhancement of

proposed algorithm which should focus on the random-generation capability of key with the key exchange process and also enhance the file sharing features of proposed algorithm based on attributes. IoT privacy and protections are the most important concern currently in academia and manufacturing. Due to resource limitation issue of IoT, accessible protection explanation is not well matched. Our planned structural design offers an explanation to the majority of the protection and solitude coercion while considering the resource limitation issue of IoT.

References

[38] P. Keikhosrokiani, N. Zakaria, N. Mustaffa, T.-C. Wan, M. I. Sarwar, and K. Azimi, Mobile Health: A Technology Road Map. Cham: Springer International Publishing, 2015, ch. Wireless N, pp. 687–726.

[39] S. R. Steinhubl, E. D. Muse, and E. J. Topol, "The emerging field of mobile health." Science translational medicine, vol. 7, no. 283, p. 283rv3, 2015.

[40] A. B. Labrique, L. Vasudevan, E. Kochi, R. Fabricant, and G. Mehl, "mHealth innovations as health system strengthening tools: 12 common applications and a visual framework." Global health, science and practice, vol. 1, no. 2, pp. 160–71, 2013.

[41] J. Barry, "Next Generation European Ambient Assisted Living Innovation Alliance: Business Model Analysis," 2013.

[42] F. Vannieuwenborg, T. Van Auwermeulen, J. Van Ooteghem, A. Jacobs, S. Verbrugge, D. Colle, and M. Pickavet, "Smart home care platforms: Where is the added value?" in 25th European Regional Conference of the International Telecommunications Society, 2014, pp. 1–27.

[43] 5G Infrastructure Association, "5G-PPP White Paper on eHealth Vertical Sector," no. September, 2015.

[44] P. Gope and T. Hwang, "BSN-Care: A Secure IoTBased Modern Healthcare System Using Body Sensor Network," IEEE Sensors Journal, vol. 16, no. 5, pp. 1368–1376, 2016.

[45] Y. J. Fan, Y. H. Yin, L. D. Xu, Y. Zeng, and F. Wu, "IoTbased smart rehabilitation system," IEEE Transactions on Industrial Informatics, vol. 10, no. 2, pp. 1568–1577, 2014.

[46] N. Zhu, T. Diethe, M. Camplani, L. Tao, A. Burrows, N. Twomey, D. Kaleshi, M. Mirmehdi, P. Flach, and I. Craddock, "Bridging e-Health and the Internet of Things: The SPHERE Project," IEEE Intelligent Systems, vol. 30, no. 4, pp. 39–46, 2015.

[47] C. F. Pasluosta, H. Gassner, J. Winkler, J. Klucken, and B. M. Eskofier, "An emerging era in the management of Parkinson's disease: Wearable technologies and the internet of things," IEEE Journal of Biomedical and Health Informatics, vol. 19, no. 6, pp. 1873–1881, 2015.

[48] 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, no. 3, pp. 14–22, 2016.

[49] G. Wolgast, C. Ehrenborg, A. Israelsson, J. Helander, E. Johansson, and H. Manefjord, "Wireless Body Area Network for Heart Attack Detection [Education Corner]," IEEE Antennas and Propagation Magazine, vol. 58, no. 5, pp. 84–92, 2016.

[50] D. V. Dimitrov, "Medical Internet of Things and Big Data in Healthcare," Healthcare Informatics Research, vol. 22, no. 3, pp. 156–163, 7 2016.

[51] I. Olaronke and O. Oluwaseun, "Big data in healthcare: Prospects, challenges and resolutions," 2016 Future Technologies Conference (FTC), pp. 1152–1157, 2016.

[52] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and Privacy for Cloud-Based IoT: Challenges," IEEE Communications Magazine, vol. 55, no. 1, pp. 26–33, 2017.

[53] T. Nakamura, T. Yokota, Y. Terakawa, J. Reeder, W. Voit, T. Someya, and M. Sekino, "Development of flexible and wide-range polymer-based temperature sensor for human bodies," 2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI), pp. 485–488, 2016.

[54] P. Narczyk, K. Siwiec, and W. A. Pleskacz, “Precision human body temperature measurement based on thermistor sensor,” 2016 IEEE 19th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS), pp. 1–5, 2016.

[55] P. Aqueveque, C. Gutierrez, F. Saavedra, E. J. Pino, A. Morales, and E. Wiechmann, “Monitoring Physiological Variables of Mining Workers at High Altitude,” IEEE Transactions on Industry Applications, vol. PP, no. 99, p. 1, 2017.

[56] A. Eshkeiti, M. Joyce, B. B. Narakathu, S. Emamian, S. G. R. Avuthu, M. Joyce, and M. Z. Atashbar, “A novel self-supported printed flexible strain sensor for monitoring body movement and temperature,” IEEE SENSORS 2014 Proceedings, pp. 1615–1618, 2014.

[57] G. Zhang, C. Li, Y. Zhang, C. Xing, and J. Yang, ``SemanMedical: A kindof semantic medical monitoring system model based on the IoT sensors,''in Proc. IEEE Int. Conf. eHealth Netw., Appl. Services (Healthcom),Oct. 2012, pp. 238_243.

[58] B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F. Bu, ``Ubiquitous dataaccessing method in IoT-based information system for emergency medicalservices,'' IEEE Trans. Ind. Informat., vol. 10, no. 2, pp. 1578_1586,May 2014.

[59] C. Doukas and I. Maglogiannis, ``Bringing IoT and cloud computingtowards pervasive healthcare,'' in Proc. Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS), Jul. 2012, pp. 922_926.

[60] N. Bui, N. Bressan, and M. Zorzi, ``Interconnection of body area networks to a communications infrastructure: An architectural study,'' in Proc. 18th Eur. Wireless Conf. Eur. Wireless, Apr. 2012, pp. 1_8.

[61] L. You, C. Liu, and S. Tong, ``Community medical network (CMN): Architecture and implementation,'' in Proc. Global Mobile Congr. (GMC), Oct. 2011, pp. 1_6.

[62] M. Wazid et al., “Design of secure user authenticated key management protocol for generic IoT network,” IEEE Internet Things J., vol. 5, no. 1, pp. 269–282, Feb. 2018.

[63] M. Z. A. Bhuiyan et al., “Dependable structural health monitoring using wireless sensor networks,” IEEE Trans. Depend. Secure Comput., vol. 14, no. 4, pp. 363–376, Jul./Aug. 2017.

[64] X. Xing, D. Xie, and G. Wang, “Energy-balanced data gathering and aggregating in WSNs: A compressed sensing scheme,” Int. J. Distrib. Sensor Netw., vol. 11, no. 10, pp. 1–12, 2015.

[65] M. Wazid et al., “Secure authentication scheme for medicine anticounterfeiting system in IoT environment,” IEEE Internet Things J., vol. 4, no. 5, pp. 1634–1646, Oct. 2017.

[66] J. Li, Y. Zhang, X. Chen, and Y. Xiang, “Secure attribute-based data sharing for resource-limited users in cloud computing,” Comput. Security, vol. 72, pp. 1–12, Jan. 2018.

[67] U. Premarathne, A. Abuadbba, A. Alabdulatif, I. Khalil, Z. Tari, A. Zomaya, and R. Buyya, “Hybrid Cryptographic Access Control for Cloud-Based EHR Systems,” IEEE Cloud Computing, vol. 3, no. 4, pp. 58–64, 2016.

[68] S. D. Bao, M. Chen, and G. Z. Yang, “A Method of Signal Scrambling to Secure Data Storage for Healthcare Applications,” IEEE Journal of Biomedical and Health Informatics, vol. PP, no. 99, p. 1, 2017.

[69] C. Y. Hung, W. C. Chen, P. T. Lai, C. H. Lin, and C. C. Lee, “Comparing deep neural network and other machine learning algorithms for stroke prediction in a large-scale population-based electronic medical claims database,” 2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 3110–3113, 2017.

[70] J. H. Abawajy and M. M. Hassan, “Federated Internet of Things and Cloud Computing Pervasive Patient Health Monitoring System,” IEEE Communications Magazine, vol. 55, no. 1, pp. 48–53, 2017.

[71] L. A. Tawalbeh, R. Mehmood, E. Benkhlifa, and H. Song, “Mobile Cloud Computing Model and Big Data Analysis for Healthcare Applications,” IEEE Access, vol. 4, pp. 6171–6180, 2016.

[72] P. Mach and Z. Becvar, “Mobile Edge Computing: A Survey on Architecture and Computation Offloading,”

IEEE Communications Surveys & Tutorials, vol. PP, no. 99, p. 1, 2017. T. T. Pham, S. T. Moore, S. J. Lewis, D. N. Nguyen, E. Dutkiewicz, A. J. Fuglevand, A. L. McEwan, and P. H. Leong, "Freezing of Gait Detection in Parkinson's Disease: A Subject-Independent Detector Using Anomaly Scores," IEEE Transactions on Biomedical Engineering, vol. PP, no. 99, pp. 1– 1, 2017.

[73] Rekhis S, Boudriga N, Ellouze N. Securing Implantable Medical Devices against cyberspace attacks. Proceeding of International Conference on Anti-Cyber Crimes (ICACC). 2017 Mar 26-27; Abha, Saudi Arabia. IEEE; 2017: 187-192.

[74] Koutli M, Theologou N, Tryferidis A, Tzovaras D, Kagkini A, Zandes D, et al. Secure IoT e-Health Applications using VICINITY Framework and GDPR Guidelines. Proceeding of 15th International Conference on Distributed Computing in Sensor Systems (DCOSS). 2019 May 29-31; Santorini Island, Greece. IEEE; 2019: 263-270.

[75] Assiri A, Almagwashi H. IoT Security and Privacy Issues. Proceeding of 1st International Conference on Computer Applications and Information Security (ICCAIS). 2018 Aug 23; Riyadh, Saudi Arabia. IEEE; 2018: 1-5.

[76] Boudko S, Abie H. Adaptive Cybersecurity Framework for Healthcare Internet of Things. Proceeding of 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT). 8-10 May 2019. 2019: 1-6.

[77] Ahmed A, Latif R, Latif S, Abbas H, Khan FA. Malicious insiders attack in IoT based Multi-Cloud e-Healthcare environment: A Systematic Literature Review. Multimed Tools Appl. 2018; 77(17): 21947-21965.

[78] Daud M, Khan Q, Saleem Y. A study of key technologies for IoT and associated security challenges. Proceeding of 2017 International Symposium on Wireless Systems and Networks (ISWSN). 2017 Nov 19-22; Lahore, Pakistan. IEEE; 2018: 1-6.

[79] Safavi S, Meer AM, Melanie EKJ, Shukur Z. Cyber Vulnerabilities on Smart Healthcare, Review and Solutions. Proceeding of Proceedings of the 2018 Cyber Resilience Conference. 2019 Jan 28; Putrajaya, Malaysia. IEEE; 2018: 1-5.

[80] J. P. Cheng, C. H. Lee, and T. M. Lin, "Prioritized Random Access with dynamic access barring for RAN overload in 3GPP LTE-A networks," 2011 IEEE GLOBECOM Work. GC Wkshps 2011, pp. 368–372, 2011.

[81] Pratas, Nuno K., et al. "Code-expanded random access for machine-type communications." 2012 IEEE Globecom Workshops. IEEE, 2012.

[82] A. Laya, L. Alonso, and J. Alonso-Zarate, "Is the random access channel of LTE and LTE-A suitable for M2M communications? A survey of alternatives," IEEE Commun. Surv. Tutorials, vol. 16, no. 1, pp. 4–16, 2014.

[83] Wu, X., Yang, E., & Wang, J. (2017). Lightweight security protocols for the Internet of Things. 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). doi:10.1109/pimrc.2017.8292779 Park, Y., & Park, Y. (2017).

[84] A Selective Group Authentication Scheme for IoT-Based Medical Information System. Journal of Medical Systems, 41(4). doi:10.1007/s10916-017-0692-9 Janbabaei, S., Gharaee, H., & Mohammadzadeh, N. (2016).

[85] Lightweight, anonymous and mutual authentication in IoT infrastructure. 2016 8th International Symposium on Telecommunications (IST). doi:10.1109/istel.2016.7881802.

[86] M. Shirvanimoghaddam et al., "Massive Multiple Access Based on Superposition Raptor Codes for Cellular M2M Communications," IEEE Trans. Wireless Commun., vol. 16, no. 1, pp. 307-319, Jan. 2017.

ISARA INSTITUTE OF MANAGEMENT & PROFESSIONAL STUDIES

WWW.IIMPS.IN

EARN YOUR

MBA



Accreditation & Ranking

UGC / NCTE Approved.

INFO@IIMPS.IN

011-41005174

RESEARCH GATEWAY

STOP PLAGIARISM

1 Submit your content in Word File.

2 Get report in 48 hrs.

3 *Missing content or references will be fixed.

4 Citation for your work.

5 Get accurate user friendly report.

researchgateway.in | info@researchgateway.in

+91-9205579779

AROGYAM ONLINE

Arogyam Ayurveda

Holistic Healing through herbs

100% NATURAL

PARIVARTAN PSYCHOLOGY CENTER

COLOR PSYCHOLOGY : HOW COLOR AFFECT YOUR CHILD

BLUE — Calms your Child's Mind & Body

YELLOW — Promotes Concentration, Stimulates the Memory

PINK — Evokes Empathy, makes your Child Calm

RED — Excites and energizes your Child's body

GREEN — Improves Reading speed and Comprehension

www.parivartan4u.com

Confuse about your children's future?

भारतीय भाषा, शिक्षा, साहित्य एवं शोध

ISSN 2321 – 9726

WWW.BHARTIYASHODH.COM

INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SCIENCE & TECHNOLOGY

ISSN – 2250 – 1959 (0) 2348 – 9367 (P)

WWW.IRJMST.COM

INTERNATIONAL RESEARCH JOURNAL OF COMMERCE, ARTS AND SCIENCE

ISSN 2319 – 9202

WWW.CASIRJ.COM

INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SOCIOLOGY & HUMANITIES

ISSN 2277 – 9809 (0) 2348 - 9359 (P)

WWW.IRJMSH.COM

INTERNATIONAL RESEARCH JOURNAL OF SCIENCE ENGINEERING AND TECHNOLOGY

ISSN 2454-3195 (online)

WWW.RJSET.COM

INTEGRATED RESEARCH JOURNAL OF MANAGEMENT, SCIENCE AND INNOVATION

ISSN 2582-5445

WWW.IRJMSI.COM

JOURNAL OF LEGAL STUDIES,POLITICS AND ECONOMICS RESEARCH

WWW.JLPER.COM