# A Review on Identification & Analysis of Security Issues and Challenges of IoT based Healthcare

**Vani G, Bharathi Malakreddy A**

***Abstract*: Healthcare applications are one of the major fields from the business user's perspective and an important domain. Healthcare applications require a degree of authentication & authorization. An Authentication is a mechanism of authorizing a particular integrity in a communication system which assures the authenticity of the element in intercommunication. It is one of the fundamental objectives of the security. In this paper, we are focusing on a multi-factor authentication method for the IoT based healthcare systems. The survey will find the multi-factor authentication related work, different types of security attacks, risk, security gaps in healthcare systems. As a result, there will be a gap that could be further investigated so that more types of authentications are feasible. The conclusion of this paper is that by using a multi-factor authentication method, there are possibilities for proposing a secured authentication and authorized algorithm for IoT based healthcare system and overviewing of sensor destruction and different types of potential attacks on IoT devices based on IoT healthcare system***

***Index Terms*: Authentication, Authorization, Multi-factor, Role-Based Access Control, data confidentiality, confidentiality, sensitivity, security attack**

## I. INTRODUCTION

Kevin Ashton in 1999 firstly composed Internet of Things about Radio Frequency Identification (RFID) which has a pre-requisite for implementing systems which were classified as IoT's. Today, healthcare applications are one of the major fields from the business user's perspective and it's an important domain [1]. An Authentication is a technique to validate an identity to certify the user prior in allowing access to the authorization and guaranteed resource of the technique to validate the authentication of the user has been acknowledged or permitted to access the requested resource

Healthcare applications necessitate a number of authentications and authorizations, few contain highly Personally Identifiable Information & Protected Health Information sensitive data that pre-requisite to control as it is changed forth and back among the desktop or mobile applications and it is server-side database or storage place. The Role-Based-Access Control (RBAC) is an applicant data for protecting most sensitive data of applications [2]. The application layer defines various applications and drivers specific services to the end user. Data confidentiality and integrity need to be assured. Authentication and authorization techniques must be applied to prevent an unauthorized access [3]. The health associated records are extremely hypersensitive and confidential entity and it is the fundamental goal of security. There are fundamental security requirements for adopting to assure the records. Typically, health related records must constantly be encrypted during transmission, even in offline approach. At present, the highly serious issues are personal confidentiality. Hence, health related personal record becomes the core for protection. In sequence to protect individual health record is one of the major tasks. Mechanism of authentication is adopted between record owner and conservator of healthcare [4-9].

## II. Authentication and Authorization in Healthcare system

**Authentication –** An Authentication is a mechanism of authorizing or certifying identity in intercommunication an assure the reliability of the source or element of the communication. Authentication is one of the preliminary objectives of the security and operates as a gateway in front of the security system to prevent the flaw. The user ID and the password submitting mechanism is the most commonly authentication used by a Secure Socket Layer (SSL). A plaintext password transmission is calculated by the Cryptography hash and avoidance. The authentication will require end users to re-authenticate every time they access resource [10]. Authentication works in two different ways. 1. Local OS and Authentication Server. The important authentication factors are Single factor authentication, Two factor authentication, Three factor authentication, one time password, biometric factor, mobile authentication continuous authentication, API authentication and open authorization [11]. The entire network is a breach in safety to protect the system from impersonating nodes of authentication is necessary to avoid illegal access. The two aspects addressing data confidentiality are data access mechanism and object authentication processes, where data is transmitted, routing and encryption that are precious to provide safety. Password authentication, Biometric authentication, and Token authentication are its different types [12].

**Authorization -** Authorization is the process of landing someone authorizing to do or have. A system administrator in a multiuser application is in allowing the user to access the system about privileges of use. Before anyone entering to the application, it wants to inspect what resources the user can be given as permission during the session.

**Manuscript published on 28 February 2019.**
***Correspondence Author(s)**
**Vani G**, Senior System Analyst, Sonata Software Ltd, Bangalore, India.
**Bharathi Malakreddy A,** Department of CSE, BMSIT&M, Bangalore, India.

So, authorization is consistently viewed as both the fundamental setup of acceptance in system administrator and the permission values is actually checked to setup when the user is getting access. MAC (Mandatory Access Control), DAC (Discretionary Access Control), RBAC (Role Based Access Control), UCON(Usage Control), CapBAC (Capability Based Access Control) and ABAC (Attribute Based Access Control) are different types of authorization modes [13].

**Confidentiality and Sensitivity-** Data confidentiality is relevant to the business applications, where only authorized person can access or modify the data. In the context of an IoT, the data confidentiality is addressed by two important aspects. The first is about the data access mechanism and a second is about object authentication processes. Sensitivity security is applied to secure high profile or risky data. A sensitivity level is assigned to the sensitive data or to the client to restrict the viewing and modification of the data to a few users [14].

## III. Types of Authentication Methods and Security Attacks in a Healthcare System

Lightweight authentication and Multi-factor authentication are the two important types of authentication methods. In this paper, we are focusing on Multi-factor authentication.

**Lightweight Authentication –** Lightweight authentication methods are used in Machine to Machine (M2M) communications in an IoT environment.

**Multi-Factor authentication** - Multi-factor authentications require more than single factors to the user which includes biometric factor like fingerprint, facial identity, possession factors such as security token key generated by the authenticator application. Multi-factor authentication (MFA) is one of the best ways to prevent unauthorized users from accessing health or medical data. It required in multiple methods of identification. In the attack key-chain, the implementation of multi-factor authentication across end-user and privileged user blocks cyber-attacks through multiple points and protect against credential compromise.

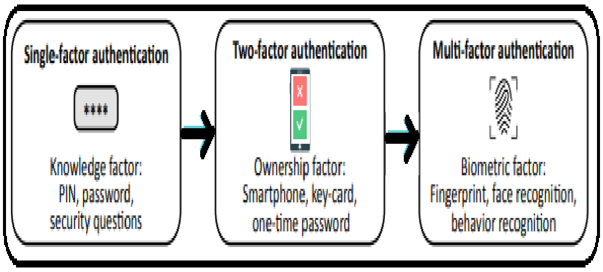
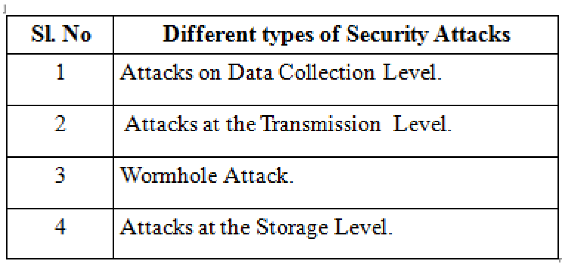


**Figure – 1 Types of Authentication methods**

Figure 1 shows the different types of authentication methods: They are a single factor which contains knowledge factor i.e. Pin, password and security questions. The second factor which is ownership as in smartphone, key card & one-time password and in a Multi-factor method as Biometric i.e Fingerprint, face identity, and behavior recognition.

The following table 1 shows the various types of attacks in security. The primary security attacks are Attacks on Data Collection Level, Wormhole Attack, Attacks at the Transmission Level and Attacks at the Storage Level [15].

**Table – 1 Security Attacks**



| Sl. No | Different types of Security Attacks |
|---|---|
| 1 | Attacks on Data Collection Level. |
| 2 | Attacks at the Transmission Level. |
| 3 | Wormhole Attack. |
| 4 | Attacks at the Storage Level. |

## IV. Overview of Sensor Destruction in Healthcare of IoT

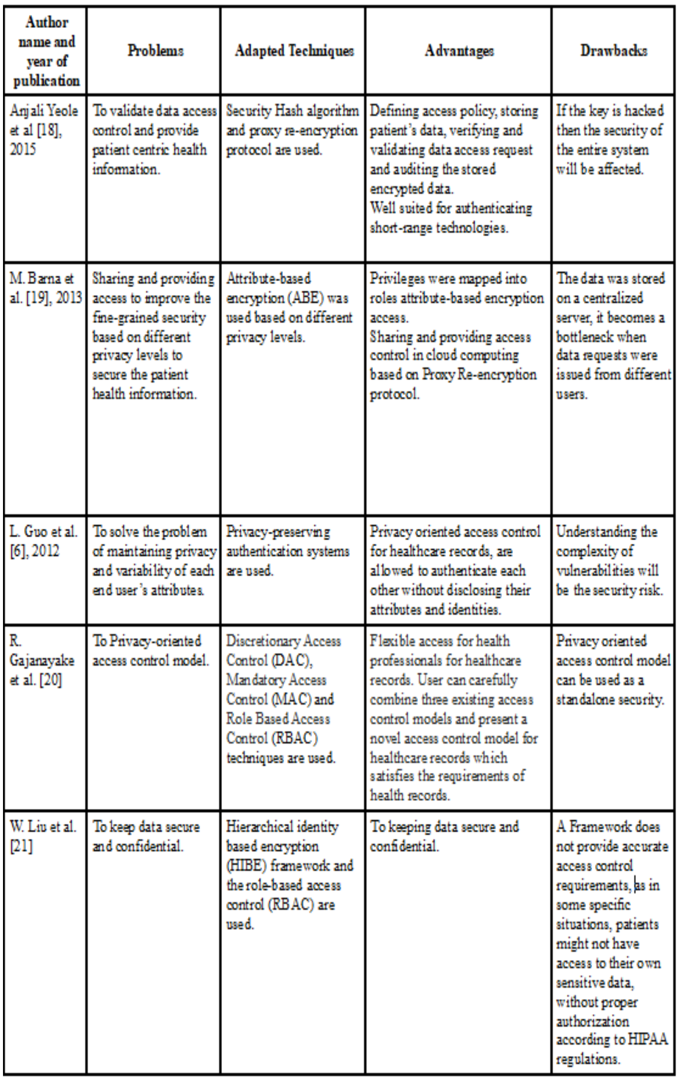
The major attacks can render during sensors are functioning unattended in rough and remote areas. Different kinds of malicious activity can attempt to disrupt, aggregate, reject, destroy and downgrade the patients secured health information itself. Attacks are classified into two categories. They are Active Attack and Passive Attack. An active attack endeavor to alter the system resources or affect its system operation and a passive attack attempts to review and do a benefit to information from the system which does not damage the system resources. The primary security fault causes serious threats to the safety of health about of the patients. Medical devices can be remotely manipulate, controlled dosage levels for drug infusion pumps. There are different types of sensor network holes. They are Routing holes, Coverage holes, Worm/Sinkholes and Jamming holes [16]. Many different sensors and approaches are there for sensor network holes to repairing the hole, preventing hole, detecting hole and avoiding hole which is capable to monitor a vast variety of ambient conditions as a movement, humidity, temperature, the presence and absence of particular kinds of objects, mechanical stress levels on attached objects. Different types of potential attacks on IoT devices based on IoT healthcare system [17]. The attacks on IoT devices are classified as:

- **Physical Attacks -**Tamper hardware components.
- **Side Channel Attacks** – Are recapturing from the encryption device.
- **Cryptanalysis Attacks** – Focused on ciphertext, try to crack the encryption.
- **Software Attacks** –The prime source of security susceptibility in any systems over its own interface communication.
- **Network Attacks** –Because the nature of the broadcast, transmission intermediate attacks are common in wireless communication systems.

## Related Work

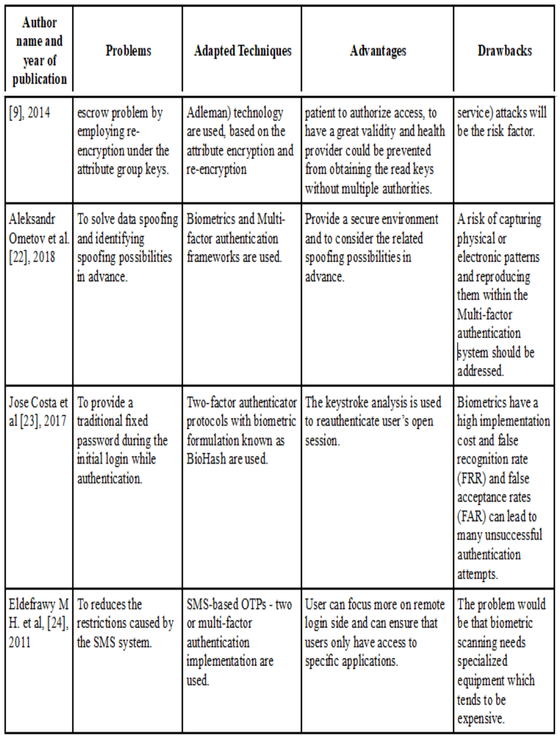
In existing work, there are many techniques that are used to secure in access control. In this below table 2 and 3, we discuss several existing proposal approaches that are applied for the security mechanism.

**Table – 2 Summary of the various possible issues and challenges in IoT based healthcare sector**



| Author name and year of publication | Problems | Adapted Techniques | Advantages | Drawbacks |
|---|---|---|---|---|
| Anjali Yeole et al [18], 2015 | To validate data access control and provide patient centric health information. | Security Hash algorithm and proxy re-encryption protocol are used. | Defining access policy, storing patient's data, verifying and validating data access request and auditing the stored encrypted data.<br>Well suited for authenticating short-range technologies. | If the key is hacked then the security of the entire system will be affected. |
| M. Barna et al. [19], 2013 | Sharing and providing access to improve the fine-grained security based on different privacy levels to secure the patient health information. | Attribute-based encryption (ABE) was used based on different privacy levels. | Privileges were mapped into roles attribute-based encryption access.<br>Sharing and providing access control in cloud computing based on Proxy Re-encryption protocol. | The data was stored on a centralized server, it becomes a bottleneck when data requests were issued from different users. |
| L. Guo et al. [6], 2012 | To solve the problem of maintaining privacy and variability of each end user's attributes. | Privacy-preserving authentication systems are used. | Privacy oriented access control for healthcare records, are allowed to authenticate each other without disclosing their attributes and identities. | Understanding the complexity of vulnerabilities will be the security risk. |
| R. Gajanayake et al. [20] | To Privacy-oriented access control model. | Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role Based Access Control (RBAC) techniques are used. | Flexible access for health professionals for healthcare records. User can carefully combine three existing access control models and present a novel access control model for healthcare records which satisfies the requirements of health records. | Privacy oriented access control model can be used as a standalone security. |
| W. Liu et al. [21] | To keep data secure and confidential. | Hierarchical identity based encryption (HIBE) framework and the role-based access control (RBAC) are used. | To keeping data secure and confidential. | A Framework does not provide accurate access control requirements, as in some specific situations, patients might not have access to their own sensitive data, without proper authorization according to HIPAA regulations. |

**Table – 3 Summary of the various possible issues and challenges in IoT based healthcare sector**



| Author name and year of publication | Problems | Adapted Techniques | Advantages | Drawbacks |
|---|---|---|---|---|
| [9], 2014 | escrow problem by employing re-encryption under the attribute group keys. | Adleman) technology are used, based on the attribute encryption and re-encryption | patient to authorize access, to have a great validity and health provider could be prevented from obtaining the read keys without multiple authorities. | service) attacks will be the risk factor. |
| Aleksandr Ometov et al. [22], 2018 | To solve data spoofing and identifying spoofing possibilities in advance. | Biometrics and Multi-factor authentication frameworks are used. | Provide a secure environment and to consider the related spoofing possibilities in advance. | A risk of capturing physical or electronic patterns and reproducing them within the Multi-factor authentication system should be addressed. |
| Jose Costa et al [23], 2017 | To provide a traditional fixed password during the initial login while authentication. | Two-factor authenticator protocols with biometric formulation known as BioHash are used. | The keystroke analysis is used to reauthenticate user's open session. | Biometrics have a high implementation cost and false recognition rate (FRR) and false acceptance rates (FAR) can lead to many unsuccessful authentication attempts. |
| Eldefrawy M H. et al, [24], 2011 | To reduces the restrictions caused by the SMS system. | SMS-based OTPs - two or multi-factor authentication implementation are used. | User can focus more on remote login side and can ensure that users only have access to specific applications. | The problem would be that biometric scanning needs specialized equipment which tends to be expensive. |

## VI. PROPOSED SECURITY SOLUTIONS FOR HEALTHCARE APPLICATIONS ON AUTHENTICATION AND AUTHORIZATION.

It's very challenging to identify and conclude all the possible attacks, vulnerabilities and threats associated with IoT based on healthcare domains. The table - 3 presents a few solutions which have been proposed in order to resolve the issue and reduce the risks [25,26,27].

## VII. CONCLUSION

In this paper, presents an overview and analysis of authentication & authorization on the Internet of Things based healthcare sector. As the authentication and authorization are the two very important security challenges in the IoT based healthcare system. Multi-factor methods are used which has several benefits in the healthcare sector, still security challenges exist. These challenges might be in the form of overcoming the authentication and authorization concerns. Few solutions are discussed in order to resolve the issues and reduce a risk. The survey paper also went through the **a**uthentication issues, multi-factor authentication and different types of security attacks, risk, security gaps in healthcare systems. There are numerous opportunities to improve to make the authentication algorithms even more secure such as Elliptic curve cryptography based mutual authentication, Keed Hash scheme without certification authority and Physical Unclonable Function (PUF) based mutual authentication to make everything even much more secure and hence that could be used to create an authentication and authorization algorithm to overall benefit the healthcare applications [26].

## ACKNOWLEDGMENT

I would like to express my gratitude to Sonata Software Ltd., for providing me a congenial environment and support at my workplace. I would like to express my sincere thanks to Dr. Bharathi Malakreddy A, Prof. Department of CSE, BMSITM, for her valuable guidance, encouragement and suggestions which helped me a lot in the completion of the paper. Last but not the least; I would like to thank my family members for their moral support and all my friends and colleague for their encouragement, help and co-operation.

## REFERENCES

1. Alok Kulkar et al, 'Healthcare applications of the internet of things– A Review', Vol.5, 2014, pp 6229-6232.
2. Dylan Sey et al, 'A survey on authentication methods for the IoT', Vol.2, 2018, pp 537-567.
3. Hafizah Che Hasan et.al, 'Comparasion of authentication methods in IoT technology', Vol. 12, No: 3, 2018
4. Lee T, "Verifier Based three party authentication schemes", Volume. 38, Number 5, in 2014, pp 464 - 472.
5. K Chen , Y Chang et.al, "Aspect oriented design and implementation of adaptable access control for Electronic Medical Record", in 2010, pp181- 203.
6. L Guo, C Zhang et.al, "A Privacy preserving attribute based authentication system for Mobile Health Networks", in 2014, pp 927 – 1941.
7. Jin .J, Ahn .G, Covington M et.al, "Access Control Model for Sharing Composite Electronic Health Records", in 2009, pp 340 - 354.

8. Burnap .P, Spasic .I , Gray .W, Hilton .J, Rana .O, and Elwyn .G, “Protecting Patient Privacy in Distributed Collaborative Healthcare Environments by Retaining Access Control of Shared Information”, in 2012, pp 490-497.
9. H. Zhou, X Lin, Dong X et.al, “Patient Self controllable and Multi level Privacy preserving cooperative authentication in Distributed MHealthcare Cloud CS', in 2014, pp.1693-1703.
10. Rafidha Rehiman K Aet.al, “A Secure Authentication Infrastructure for IoT Enabled Smart Mobile Devices”, in 2016, in Volumel 9, DOI: '10.17485/ijst/2016/v9i9/86791'.
11. Lella . A; Martin B et al, “The Mobile App Report. available at – www.comscore.com/Insights/Presentationsand-Whitepapers”, in 2015.
12. Anurag Shukla, “A Survey on Next generation Computing IoT Issues & Challenges”, in ‘International Journal of Pure and Applied Mathematics’', Vol.118, No.9 2018, pp 45-64.
13. Hafizah Che Hasan et al, “Comparison pf authentication methods in IoT technology”, Vol.12, pp 3, 2018.
14. Shantha Mary, Joshitta R and Arockiam, 'Authentication in Internet Of Things Environment: A Survey', Vol 6, Issue 10, Cotober 2016, ISSN:2277 128X.
15. Isra Ahmed Zriqat, 'Security and Privacy Issues in Ehealthcare systems - Towards trused services', Vol. 7, pp 9, 2016.
16. Afaa Jabenur, Nabil Sahli et.al , “Survey on Sensor holes: Acause effect solutions perspective”, in procedia CS, Doi10.1016/J.Proces.2013.06.151
17. Somasundaram Ragupathy and Mythili Thiruganantam, “IoT in Healthcare: Breaching security issues”.
18. Anjali Yeole, Sadaf Ahmedi et.al, “A Robust Scheme for Secure communication in IoT”, in International Research', Volume 3, no.11, 2015, pp 10401- 10406.
19. Barna M , “Ciphertext policy attribute based encryption', pp 497-628. doi: 10.1038/nature12157, Epub 2013 April 28.
20. Gajanayake R, Sharma et.al, “Privacy oriented access control for Health records”, in 'Electronic health information journal', 2014, pp 5.
21. W. Liu et , “Cryptography”, in third IEEE International Conference, Pune, India August 2017, IEEE. Available online at 'ieeexplore.ieee.org/Xplore/home.jsp'.
22. Ometov, Aleksandr et al, “Multi-Factor Authentication - A Survey Cryptography”, vol. 2.
23. Jose Costa, “A Two Factor Authentication scheme”, DOI: 10.13140/RG.2.2.16228.99207, Jun 14, 2017
24. Kennedy. Eand Millard .C, “Data security & Multifactor authentication ' in “Computer Law & Security Review”, Volume: 32, Number 1, 2016, pp 91 - 110.
25. Camenisch J, Fischer S et.al, 'Privacy andidentity management for life', in 'Springer Science & Business Media', 2011.
26. Eldefrawy M.H; Alghathbar K et.al 'OTP based two factor authentication using mobile phones', in 8 International Conference on IT, April 2011, pp 327 - 331.
27. Bruce Ndibanje; Hoon-Jae Lee et.al “Security Analysis and Improvements of Authentication and Access Control in the IoT', in Volume 14, 2014, pp 14786 -14805.
28. Jose L; Hernández Ramos; Antonio J; Skarmeta et al, “Distributed Capability-Based Access Control for the IoT”, in Vol: 3, Number 3/4, 2013, pp.1-16.
29. Bruce Ndibanje , Hoon-Jae Lee, and Sang-Gon Lee, ‘Security Analysis and Improvements of Authentication and Access Control in the Internet of Things’, Sensors, Vol. 14, 2014, pp 14786-14805.
30. Muhammad, K.R.R.S.; Lee S: Lee Y.K. 'Biometric Based Distributed Key Management Approach for Wireless Body Area Network. Sensors”', in 2010, Vol: 10, pp. 3911-3933.
31. Sanaz Rahimi Moosavi et.al “SEA – A Secure & Efficient authentication and authorization architecture for IoT based Healthcare using Smart gateways”, in Procedia CS Journal, published in Elsevier in 2015, Vol.52, pp. 452-459
32. Vani.G, Bharathi Malakreddy.A, “Security challenges in Internet of Things in Healthcare Domain”, in September 2016 ,DOI No. IAECS IRAJ DOI 5592,pp.141-144.
33. Vani.G, Bharathi Malakreddy.A, “ Survey on Security challenges in IoT in Healthcare domain”, in ICNTET, 2018,ISBN-CFP18P34-PRT/978-1-5386-5629-7.

*Published By:*
*Blue Eyes Intelligence Engineering*
*and Sciences Publication (BEIESP)*