Persuasive Factors and Weakness for Security Vulnerabilities in BIG IOT Data in Healthcare Solution

Madhu Sharma Gaur1, Sanjeev Kumar2, Navneet K Gaur3, Prem Sagar Sharma4
1,3,4 G. L. Bajaj Institute of Technology and Management, Greater Noida, U,P India
2Program Manager at Telus International, Noida, India

e-mail: 1madhu14nov@gmail.com, 2sanjeevnmc83@gmail.com,
3navneetkg@gmail.com, 4premsagar1987@rediffmail.com

Abstract. In the present scenario, public health is a global challenge. In view of COVID-19 pandemic, interventions of emerging technologies has been highly increased and post-pandemic big technological shift is expected for providing information and communication Technology-enabled solutions to healthcare as well a meeting other social challenges. Internet of Things or IoT and Big data are the technologies prominently being used in healthcare applications. In smart city visualization to provide ubiquitous computing environment, urge of smart, small but powerful sensor devices or IoT technology-enabled healthcare solutions deployments done over open networked infrastructure and underlying architecture. Such highly dynamic and heterogeneous environment with rapid digital transformation enforcing trusted security resource-restrictions and performance implication. In this paper, firstly, we explore the existing security, privacy and authentication weakness in reference to IoT or IoMT and big data enabled healthcare applications. Secondly, scaling the low to high security risks done based on the major weaknesses. In this work primarily we focus on most challenging attacks like Denial of Services (DoS), Man in the middle and dynamic intrusions. In winding-up machine learning based intelligent adaptive approach proposed for underlying deficiencies and insufficiencies in IoT enabled Healthcare application security. The key driving forces for the imprecision of trust and security with emerging Big IoT also presented as future scope.

Keywords: Bigdata, Healthcare, Internet of Things (IoT), Machine Learning, Security

1. INTRODUCTION
Internet of Things or IoT is a heterogeneous and distributed network of embedded sensor devices communicating through wired or wireless communication technologies [1]. With IoT devices, not only world become more connected to bring great advantages but also bring new security challenges with new threats and vulnerabilities. Big IoT Data identified as a significant elucidation to alleviate the Information and Communication Technology (ICT) enabled healthcare. There are many existing research [2-5] focused on IoT system security with Big Data based healthcare systems too. There is no standard IoT architecture to be followed in all applications and technologies. Although in the year 2018 and 2019 IEEE proposed has IoT architecture framework for smart cities and smart grid [6-7.]

In
the healthcare landscape, day-by-day number of connections and access of variety of devices between objects and human beings are rapidly growing.

IoT devices are resource-restricted and less secure where e-healthcare solution is human-centric system and ensuring security is prime concern. Immediate healthcare concerned actions are always on high priority, therefore access of data and services with low or now security assurance system becomes prone. Meanwhile attackers and intruders target IoT devices and track the data with location and due to attacks and threats device or system behave maliciously. In view of enforcing rapid development and fast deployment of technology enabled healthcare solutions, exchange of healthcare data and voluminous Big Data analytics between patient and other stakeholders leading to unknown security attacks and threats. Variation in IoT devices to provides variety of healthcare applications and services are expanding beyond the mere things or objects. Even attempts are being done to implant IoT devices into the human body to monitor the live conditions [8]. New threats are consistently increasing and community researchers constantly working to provide end-to-end secure digital transformation. As per recent advancement in IoT based healthcare application, an open source application OpenAPS [9] developed using artificial pancreases system for continuous monitoring of glucose level in diabetes patients.

In the smart healthcare Big Data analytics is also a buzzword and revolutionizing the health informatics analysis. In view of smart grid applications of Big Data and associated security concerns has been discussed in [10]. A survey on deep learning for IoT and Big Data with streaming analytics had done [11]. In healthcare Big IoT data in variety collected from different sources and always have potential security risks like

- Stakeholders compromised behavior and identifying factitious data
- High volume of dynamic data from different sources
- Security risk prediction and Trusted data analysis
- Twisted interpretation and inappropriate conclusions from novel set of voluminous data with or without security assurance
- Miss-Extraction and Misclassification of Data

Rest of the paper organized as next part present the related work explored specifically in subjective area of research privacy and security. In the third section, security apprehensions in Big IoT data enabled applications discussed to identify the security weaknesses with underlying deficiencies. In the IV part our proposed work has been presented and in the last comparative analysis followed by conclusion and future work discussed.

2. RELATED WORK
   As a part of explorative research approach, primarily related existing literature explored. There are several research papers, white papers, articles and blogs highlighting the Big IoT Data security. A comprehensive survey of IoT in healthcare has been presented in [12]. Similarly from Micro to Nano evolution of wireless sensor based healthcare has been done in [13]. Another comprehensive study of security in Internet of Things [14] was also done where three reference model presented with motivation of attackers in new paradigm discussed. Further security attack in IoT based application has been discussed where a survey on building blocks reference model [15] has been done. Machine learning and predictive Modelling in the healthcare research is revolutionizing the way health data are being collected used and analysed. These are the wide spread technologies offering risk prediction, diagnosis, prognosis patients healthcare data analysing [16]. On the other side of this sensitive human-centric complex healthcare application accessing Big Data from dissimilar IoT devices raises security concerns for researchers. In the different IoT enabled application domains improvements in traffic, manufacturing and healthcare has been discussed with business scaling security evaluation is needed. [17]. Privacy in view of smart city applications discussed in [18] where security and privacy are represented as separate stream with increase of cyberspace and cyber systems. A key establishment scheme using secure signature based authentication for IoT applications was proposed in [19]. Big Data in cloud environment for secure storage and verification scheme SecSVA has been presented in [20].

In context IoT and IoMT (Internet of Medical Things) analysis of cyber risks, holistic analysis of assessment, frameworks, vectors and risk ranking process presented in [21]. A lightweight IoT based
authentication scheme has been proposed in [22] in view of cloud computing. Another multi-factor lightweight biometric based remote user authentication and key agreement scheme used for IoT security [23]. This scheme uses reasonable resources for one-way hash function and XOR operation that makes it suitable to resource restricted IoT security. It provides strength, against several security attacks through AVISPA tool but it require testbed setup for applying in real world IoT based systems and to understand memory requirements as well.

Despite of continuous efforts of researchers’ providing trusted security is always a thrust area, Security issues are still challenging. In the past year 2019 significant research on has been done to explore and identify the security threats and solutions, Intrusion detection, network or router attacks [24-32] in IoT architecture and technology deployment, Security in healthcare is more critical and due to day today rising security attacks and threats along with IoT devices and application complexity expansion, privacy, authentication and access control are the big concern for ensuring security in IoT enabled world of healthcare.

Key Contribution of this paper defined in many folds; one explores the existing security, privacy and authentication weakness in reference to IoT or IoMT and big data enabled healthcare applications. Secondly, scaling the low to high security risks done based on the major weaknesses. In this work, primarily we focus on most challenging attacks like Denial of Services (DoS), Man in the middle and dynamic intrusions. In winding-up machine, learning based intelligent adaptive approach proposed for underlying deficiencies and insufficiencies in IoT enabled Healthcare application security. The key driving forces for the imprecision of trust and security with emerging Big IoT also presented as future scope.

Research Methodology: A systematic review of existing related research done to identify the weakness of security risks of IoT and Big Data risks. Primarily we have explored IEEE Xplore, ScienceDirect, ACM, Digital Library, and Springer research papers, white papers, domain expert articles to identify the subjective area weaknesses and summarized the risks with in the scale of low to high security itself is a wide area of concern. As a part of Inclusion and exclusion, criteria in this paper we have focused particularly on privacy and authentication in association with IoT and Big Data enabled Healthcare applications deployment. Research papers with respect to the recent years describing about IoT, Big Data, security, healthcare with privacy authentication has been mainly focused and reviewed.

3. SECURITY APPREHENSIONS BIG IOT HEALTHCARE APPLICATION

High expansion of IoT or IoMT devices and collected Big Data complexity, ensuring security in e-healthcare deployment with resource restrictions and performance implications are still challenging. IoT and medical devices are rising with security apprehensions. Trust and Security assurance is necessary to enhance the confidence and adoption of the ICT enabled system. Here data security is critical; a system must bide on some specific evidence to meet the necessary requirements for trusted security. Existing IOT enabled healthcare solutions and underlying approaches developing and deploying security techniques to detect attacks, threats and other vulnerability regardless of much consideration of security requirements alignment with solution objectives. As per HIPPA journal report of March 2019 healthcare data breach [33]. As shown in figure 1. In general the organizations and their operational teams usually don’t have much control over the core technicality of hardware, software with IoT deployments, thus unable to critically contemplate the security concerns while operational statuette.
As per Gartner Survey security [34] and Trusted hardware is the most demanding and crucial area of concern for deployment of IoT systems. As per Mr. Jones, by the Year 2023 deployments of hardware, software with secure and trustworthy IoT expected to see and advised CIOs to collaborate with chief information security experts to ensure right staff and involvement in purchasing of IoT devices and embedded operating systems. For Security leaders emerging technological shift and risk assessment are the biggest challenges. Usually security managers are case-hardened to consider calculated risks and mitigating assessed threats or attacks thus further deployments with IoT devices introduces new security parameters and measures over traditional mechanisms. In the human-centric critical applications like IoT enabled healthcare application integrated approaches can result better security assessment and adoption of new strategies with pervasive presence and acknowledgement secure and trusted operation in the digital transformation and smart operations.

4. BIG IOT DATA IN HEALTHCARE

Adoption of IoT and Big Data in healthcare is rising with potential advantages of connected healthcare. Smart and connected healthcare with IoT and Big data exaggerate multidimensional the benefits like
- Healthcare diagnosis, remote monitoring, wearable and artificial organ support
- Real time medication tracking, remote vital parameters monitoring, data collection and sharing
- Immediate and Effective Treatment
- Comprehensive record keeping and Big data analytics
- Better efficiency by automatic capturing of healthcare informatics and observations.
- Operational automation at third party level for lab reports, billing invoicing, insurance etc.

Security in healthcare defined as corporeal, technological and managerial defends to secure assets, patients, and protection of health data from erratic and unnecessary access or disclosures. Big Data is a voluminous complex data set/ It has several big characteristics like Big Volume, Big Variety, Big Veracity and Big Velocity [35]. It becomes an asset for industry and healthcare as a strategy enabler for insights prediction and better decision making.

5. PERSUASIVE FACTORS FOR SECURITY VULNERABILITIES

Along with rapidly growing technology advancements there are potential distressing counterparts associated with trust and security while using the open and dynamic environment with IoT, ensuring security is highly sensitive for healthcare data As per a recent research report [36] full 98% of IoT device traffic is unencrypted and exposing personal and confidential information as shown in figure 2.

Healthcare provider are always seeking data integrity, privacy and security assurance with trustworthiness, in spite of that day by day breaches have increased in prevalence and destruction[37-40]. Security Gaps in IoT [41] always put concern on the way of healthcare data management for service providers and researcher’s security concerns are always over data integrity, privacy and sharing among allegations that vast healthcare database creation with medical records was being rushed through without clarifying to patients and taking care of security implications.
Fig2: Full 98% of IoT Traffic is Unencrypted

It was an example quoted here but there are so many unknown cases being actually reported where security being exploited of the potential healthcare big data. Rapidly growing such cases needs the attention of all the healthcare stakeholders.

| Persuasive Factors       | IoT and Big Data Architectural                  | Security Vulnerabilities                                                                 |
|--------------------------|-----------------------------------------------|------------------------------------------------------------------------------------------|
| Rapid Deployments        | Heterogeneous Environment                     | Low or no Enforcement of security evaluation practices                                     |
| Operational Constraints  | Resource-Constrained Devices                  | Device level Security Management, Low memory, power and CPU cycle vs effective authentication |
| Lack of Software updates | Stack of Multiple technologies and rapid Expansion. | Anti-virus or security software updates at software, hardware and firmware level             |
| Lack of Security Experts | Healthcare practitioners are usually give low or no attention for upgrading ICT Technical staff | Low or no security consciousness and lack of security associated practices and trainings unknowingly leave holes for security breaches or threats. |
| Complicated Usage scenarios | Voluminous and variety of Data Or Big Data     | Hard to comply with complexity                                                              |

6. INTELLIGENT SECURITY USING MACHINE LEARNING TECHNIQUES

Data analytics and predictive modelling techniques and strategies are expected to provide better security risk assessment and trustworthy usage rather than increasing solutions only. Healthcare providers also realized that combining medical data with predictive analytics, machine learning, artificial intelligence or natural language processing, changes in the way of patient treatment has been seen and hoped that ultimately it can lead to better outcomes for all. Similarly security and trust implications on healthcare solutions can result meaningful outcomes and decision making for managing security challenges. In place of traditional security systems based on cryptography and complex encryption-decryption mechanisms guaranteed availability and accessibility to only and only authentic users. Convergence of traditional healthcare practices, vulnerable behaviour to make an intelligent training and learning based adaptively encryption and authentication process can handle security and
privacy vulnerability more reliably and effectively. Anywhere any time access of healthcare information to practitioners and patients for analysing trends in disease and treatments also open many holes for security gaps. In Big IoT data security with optimised resource utilization machine learning can help to build an intelligent security mechanism.

7. SECURITY WEAKNESS
HIPPA also dictate [42] healthcare security but compliance is not enforced. Also there are several elementary fissures observed that are making more vulnerable.

Table 2: Security pitfalls and Compliance Enforcing Challenges

| Sr.No. | Elementary Fissures            | Security Weakness                                                                 | Enforcing Challenge                                                                 |
|--------|--------------------------------|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| 1      | HIPPA Regulons                 | Healthcare Applications are not strictly following the HIPPA regulation and security Consideration. | • Make security compliance legal  
• Stopping Privilege Escalation  
• No escalation of sensitive data exposure. |
| 2      | Buying technology alone No standard security Assurance mark | IoT or Sensor medical devices are vulnerable to attacks by design or deployment. Manufacturers keep security after thought of device functional objective where tight timeline leaves security fragile. Low or no privacy testing at device design level | • Enforcing regulations to market IoT devices only after security standard mark.  
• Security by Design with Technology development |
| 3      | Miss-Configuration at server, cloud or APIs | Risk mitigation as a prime concern. More Insider leaks leads to external endpoints threats and malwares. Application Programming Interface (API) is sets of protocols to govern data sharing may leave holes for insecure access. | • Only secure session management  
• Imposing well tested periodic backup and recovery plan to control the ransomware kind of attacks increasing exponentially presently.  
• Enforcing Certification process for Open APIs.  
• Strict Evaluation of Security Settings at APIs open |
|   |   |   |
|---|---|---|
|   | Encryption is on Rest | Weak authentication code and incomplete test cases where asymmetric Bulk of Information may lead to checks on accuracy and completeness as part of quality of data |
| 4 |   | • NIST approved Cipher suits like AES, Strong Hash like SHA256 or TLS1.2. • Two or multi Factor Authentication • Secure Key Management • Enforcing Evaluation criteria |
|   |   |   |
|   | Context Awareness | IoT in healthcare with context aware adoptability of service, computing context, user context, physical context, temporal context and context history checks. |
| 5 |   | Incorporating contextual security with: • Social: Identification of people near the user • Functional: Tasks the user is running • Location: The geographical position of user • Temporal: Temporal context defined • Motivating: The reason of running task |
|   |   |   |
|   | Privacy and Protection | More open surface for attacks at hospitals Insider Threats leading to huge Security Risks and organization putting as Cyberattacks. Lack of effective management and control policies without imposing best practices for regular security verification and validation. |
| 6 |   | • Weak Authentication code and incomplete test cases • Low or no privacy testing at device design level • Asymmetric Bulk of Information • Quality of Data |
8. PROPOSED WORK

Here Machine learning can play important role to recognize the compromised behaviour/patterns to detect attacks and threats on massive devices and data sets at all on the machine speed. Machine learning identifies high-risk users and trusted users. In the critical applications like healthcare where sophisticated threats and attacks needs to monitored and detected by analysing authentication process with device and user profiling. An additional element Intelligence unified to decide action acceptance and rejection with maintaining the tracking log to alert security team for further countermeasures. The adaptive authentication with machine learning to provide better privacy and data protection with contextual role based action. In the system, each device and user while registration as unique ID, used to identify and track the malicious behaviour. In view of resource restricted small sensor or IoT devices On the other side the more a user or device profiling will be strongly matched the level of trust will be high to gain the access. In case any vulnerable pattern detected, user or device access automatically disrupted. Here we focus on the following most common and challenging vulnerabilities:

i. Denial of services attacks: One of the most common attack where large number of messages frequently with new connections transmitted for load testing and scalability of services and attackers take advantages of that. e is one of the most common attacks on the Internet [31]. In the case of

ii. Man in the middle attack in which intercepting of the message between communicating end points like sensor IoT devices and broker, attempt to altered

iii. Dynamic Intrusion detection: From port to externa attackers using special symbols or code knowing current available information for dynamically identifying which data is out of context of the current system.

The low cost information tracked as a part of parameters of adaptive authentication key components without user or device disruption. Although Parameters may altered in context of application or service access like in case of patient in healthcare, any bio feature or vital parameters can be also mapped

**Intelligent Approach Security:** In this work we propose a novel intelligent adaptive security strategy in view of IoT based healthcare application with big data analytics to detect vulnerable behaviour while accessing any device. Two factor or multifactor authentication could not sufficient to handle evolving attacks and threats. In the highly complex and connected IoT world it is quite critical to manage all the embedded sensor and IoT devices over mobile or wireless network and underlying architecture. This is an intelligent authentication where fusion of authentication and impulsive behaviour tracking and observation value determine the security level and allow deciding to accept or reject the node secure communication.

Parameters $P_1$-$P_n$ are Boolean variables will be denoted for every passed parameter is 1 and fail is denoted by 0. Proposed Machine Learning based Adaptive Encryption we use Support Vector Machine (SVM) lightweight LEA and SPEK cipher text encryption in python. Adaptive authentication provides additional multifactor authentication without user intervention.

|   | Negligence of Healthcare devices inclusion in ICT security programs | Low or no inclusion of Industrial control systems and healthcare devices in ICT Security plans | • Lack of enforcing Evaluation criteria | • IoT medical devices are communication endpoint thus organizations need to keep them under ICT security plans to control and manage expected concerns. |
|---|---|---|---|---|
| 7. |   |   |   |   |
### Table 3: Intelligent Adaptive Security Parameters

| No. | Adaptive Security Parameters |
|-----|-----------------------------|
| P1  | Device Unique Id device profiling while device registration |
| P2  | User ID Unique Authentic Id matching with predefined |
| P3  | Contextual Role Mapping |
| P4  | OTP generation in case new IP used |
| P5  | Hit/miss ratio of login attempts |
| P6  | User activity tracking with predefined role tracking |
| P7  | Session Timings as per authentic schedule |
| P8  | Bio-feature mapping |

It will automatically check vulnerable activity and maintain the log to detect malicious behaviour. This intelligent adaptive authentication will work silently in background. Machine learning based algorithm will be used to get learning based on behaviour pattern and classify the passing or failure activity. On progressive repetitive attempts it will predict the performance of adaptive authentication. In General supervised unsupervised and reinforcement learning is used where SVM, K-means, KNN and deep earning are being preferred in view better performance prediction. In this proposed model an intelligent security Manager will maintain log and generate alert in following situation.

1. Log Entry of any potential insider threat based on adaptive pattern
2. Identification of any anonymous activity
3. Detection of the potential risks with the level of fragility
4. Outsider and Insider attackers valid access credentials or invalid access which bypass the predefined Contextual roles

In the proposed approach we use SVM and KNN algorithms to predict performance for implementing lightweight encryption algorithms AES Blowfish, RC6 and SPEK encryption implementation with collision detection dynamic technique hashing. Based on adaptive parameters input text 64, 128 or 256 bit with a random key generator process given below

**Key Generator**

**Input:** Initial input as number 1’s from P1-Pn pass cases

\[ P \rightarrow \text{Vulnerable} \ (P, P_n) \]

**Output:** Key K

**Step 1:** Start

**Step 2:** Take two random numbers \( R_1 \) and \( R_2 \)

**Step 3:** Transform \( R_k = R_1^2 + R_2^2 + P \)

   Where \( P \) is the most vulnerable security parameter

**Step 4:** Add \( R_1 \) and \( R_2 \) and store in \( R \)

**Step 5:** Convert \( R \) and \( R_k \) into binary.

**Step 6:** Apply XOR on \( R \) and \( R_k \) and assign to \( K \)

**Step 7:** Apply addition modulus 10 on \( R_k \) and assign to \( K \)

**Step 8:** Stop.

An IoT healthcare is resilient to insider attacks: Insider privileged users. In this adaptive approach while access requests authentication process done through passing one by one multiple factors where silent Intelligent machine learning based security manager using SVM and KNN algorithms are used to analyse and classify the access request compromised behavior based on vulnerable two or more parameters to validate authentication action and log management. For each authentication of a device in each login attempt and access movement and behavior log will be recoded. On the collected data machine learning algorithms will be applied. in the System there will be a access log dataset that will be maintained adaptively for each attempt and based on the device of user actions vulnerability will be detected adaptively as per the training and learning process and accordingly a key will be generated for
encrypted data exchange using encryption algorithm selected randomly from the set of a lightweight Encryption algorithms with optimized resources.

Performance Evaluation: For performance evaluation we setup an environment in Lab view and anonymously vulnerable and non-vulnerable access requests where about 28 IoT devices used and in total 200 access attempts were made. Collected data set has been processed using SVM and KNN algorithms to predict performance for implementing lightweight encryption algorithms AES. Based on adaptive parameters input text 128 bit with a random key generator process given below in the table 4. Further AES variations and other lightweight encryption algorithms like Blowfish and RC6 with variable text input of 64, 128 and 256 bit testing is work in progress with collision detection dynamic technique hashing.

An IoT healthcare is resilient to insider attacks: Insider privileged users. In this adaptive approach while authentication one by one multiple factor will be analyzed to validate authentic action for authentication of a device in each login attempt and access movement

Advantages: To make this proposed approach different in fighting against compromised Security tackling following actions tracked.

• Uninterrupted Authentication Tracking: This Adaptive Approach will work silently in background without user interruption and to make it frictionless.
• Better Identity Confidence: All the login and access attempts will be evaluated to ensure only authorized users access grant.
• Customized Authentication: Based on the Contextual roles and risks access control parameters can be redefined to leverage adaptive authentication process beyond the two factor or fixed multifactor authentication.
• Minimizing the application surface holes to reduce attacks and threats

| ML Classifier | Accuracy | T 0 Test | F Test |
|---------------|----------|----------|--------|
| SVM           | 98.97    | 0.039    | 0.038  |
|               | 98.95    | 0.040    | 0.039  |
|               | 98.98    | 0.039    | 0.039  |
| KNN           | 99.81    | 0.042    | 0.039  |
|               | 99.84    | 0.041    | 0.038  |
|               | 99.87    | 0.042    | 0.039  |
• Security Risk Analysis: Big data collection and access give roots to security risk analysis to provide an intelligent engine to deal coarse threats.
• Better decision making through Intelligent Identity.

9. CONCLUSION

In this paper, survey based analysis of healthcare IoT devices authentication and privacy with security breaches has been presented. Further realization of persuasive security vulnerability forces and elementary fragility with challenges and enforced action discussed. We proposed an intelligent approach using machine leaning SVM and KNN methods in the IoT based healthcare a where data analytics and security requirement relevance has been focused to detect vulnerability we proposed machine learning based Intelligent adaptive authentications approach and performance evaluated using KNN and SVM classification algorithms to classify the access vulnerability for securing IoT based Healthcare. Testing with other Machine learning based algorithms and refining authentication process is our work in progress.

REFERENCES

[1] D.E. Kouicern, ABOuabdallah, and H lakhlef, “Internet of Things Security: a Top down survey”, Computer Networks, vol 141, pp 199-221, 2018.
[2] 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.
[3] 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.
[4] D. V. Dimitrov, “Medical Internet of Things and Big Data in Healthcare,” Healthcare Informatics Research, vol. 22, no. 3, pp. 156–163, 7 2016.
[5] C. C. Y. Poon, B. P. L. Lo, M. R. Yuce, A. Alomainy, and Y. Hao, “Body Sensor Networks: In the Era of Big Data and Beyond,” IEEE Reviews in Biomedical Engineering, vol. 8, pp. 4–16, 2015.
[6] IEEE Draft Standard for an Architectural Framework for the Internet of Things (IoT), Stan-dard IEEE P2413/D0.4.4, Dec. 2018, pp. 1–264.
[7] IEEE Draft Standard for an Architectural Framework for the Internet of Things (IoT), Stan-dard IEEE P2413/D0.4.6, Mar. 2019, pp. 1–265.
[8] G. Yang, M. Jiang, W. Ouyang, G. Ji, H. Xie, A. M. Rahmani, P. Liljeberg, and H. Tenhunen, “IOT-based remote pain monitoring system: From device to cloud platform,” IEEE journal of biomedical and health informatics, vol. 22, no. 6, pp. 1711–1719, 2018.
[9] A. Chakraborty, S. Zavitsanou, T. Soupizanarin, F. J. Doyle III, and E. Dassau. “Getting IoT-ready: The face of next generation artificial pancreas systems,” in the book chapter, The Artificial Pancreas: Current Situation and Future Directions, R. S. Sanchez-Pena and D. R. Chernavsky, Editors, Elsevier, 2019.
[10] E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, and M. S. H. Sunny, “Application of big data and machine learning in smart grid, and associated security concerns: A review,” IEEE Access, vol. 7, pp. 13960–13988, 2019.
[11] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, “Deep learning for IoT big data and streaming analytics: A survey,” IEEE Commun. Surveys Tuts., vol. 20, no. 4, pp. 2923–2960, 4th Quart., 2018.
[12] S. M. R. Islam, D. Kwak, H. 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.
[13] S. Sarkar and S. Misra, “From Micro to Nano: The Evolution of Wireless Sensor-Based Health Care,” IEEE Pulse, vol. 7, no. 1, pp. 21–25, 2016.
[14] A. Mosenia and N. K. Jha, “A Comprehensive Study of Security of Internet-of-Things,” in IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586-602, 1 Oct.-Dec. 2017, doi: 10.1109/TETC.2016.2606384.
[15] H. Akram A. Ghani and D. Konstantas and M. Mahyoub, “A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model”, International Journal of Advanced
M. Chen, Y. Hao, K. Hwang, L. Wang, and L. Wang, “Disease prediction by machine learning over big data from healthcare communities,” IEEE Access, vol. 5, pp. 8869–8879, 2017.

V. S. Shridhar, "The India of Things: Tata Communications’ countrywide IoT network aims to improve traffic, manufacturing, and healthcare," in IEEE Spectrum, vol. 56, no. 2, pp. 42-47, Feb. 2019, doi: 10.1109/MSPEC.2019.8635816.

Eckhoff and I. Wagner, "Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions," in IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 489-516, Firstquarter 2018, doi: 10.1109/COMST.2017.2748998.

S. Challa, M. Wazid, A. K. Das et al., “Secure signature-based authenticated key establishment scheme for future IoT applications,” IEEE Access, vol. 5, pp. 3028–3043, 2017.

G. S. Aujla, R. Chaudhary, N. Kumar, A. K. Das, and J. J. P. C. Rodrigues, “SecSVA: secure storage, verification, and auditing of big data in the cloud environment,” IEEE Communications Magazine, vol. 56, no. 1, pp. 78–85, 2018.

Kandasamy, K., Srinivas, S., Achuthan, K. et al. “IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process”. EURASIP J. on Info. Security 2020, 8, 2020. https://doi.org/10.1186/s13635-020-00111-0

L. Zhou, X. Li, K.-H. Yeh, C. Su, and W. Chiu, “Lightweight IoT-based authentication scheme in cloud computing circumstance,” Future Generation Computer Systems, vol. 91, pp. 244–251, 2019.

P. K. Dhillon and S. Kalra, “A lightweight biometrics-based remote user authentication scheme for IoT services,” Journal of Information Security and Applications, vol. 34, pp. 255–270, 2017.

V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A survey on IoT security: Application areas, security threats, and solution architectures,” IEEE Access, vol. 7, pp. 82721–82743, 2019.

M. Fahim and A. Sillitti, “Anomaly detection, analysis and prediction techniques in IoT environment: A systematic literature review,” IEEE Access, vol. 7, pp. 81664–81681, 2019.

T. Nandy, M. Y. I. B. Idris, R. M. Noor, L. M. Kiah, L. S. Lun, N. B. A. Jumaat, I. Ahmedy, N. A. Ghani, and S. Bhattacharyya, “Review on security of Internet of Things authentication mechanism,” IEEE Access, vol. 7, pp. 151054–151089, 2019.

K. Riad, R. Hamza, and H. Yani, “Sensitive and energetic IoT access control for managing cloud electronic health records,” IEEE Access, vol. 7, pp. 86384–86393, 2019.

N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, “Network intrusion detection for IoT security based on learning techniques,” IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2671–2701, 3rd Quart., 2019.

A. Raoof, A. Matrawy, and C. Lung, “Routing attacks and mitigation methods for RPL-based Internet of Things,” IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1582–1606, 2nd Quart., 2019.

S. Hajheideari, K. Wakil, M. Badri, and N. J. Navimipour, “Intrusion detection systems in the Internet of Things: A comprehensive investigation,” Comput. Netw., vol. 160, pp. 165–191, Sep. 2019.

J. Harrop and P. Harrop, “Internet of Things (IoT) 2017–2027: Things that think: IP ad-dressed sensor node systems,” IDTechEx Res., Tech. Report,https://www.idtechex.com/en/researchreport/internet-of-things-iot-2017-2027/499

M. Frustaci, P. Pace, G. Aloi, and G. Fortino, “Evaluating critical security issues of the iot world: present and future challenges,” IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483–2495, 2018.

R. Irons-Mclean, A. Sabella, and M. Yannuzzi, “IoT and security standards and best practices,” in Orchestrating and Automating Security for the Internet of Things: Delivering Advanced Security Capabilities from Edge to Cloud for IoT Book. Indianapolis, IN, USA: Cisco Press, Jan. 2019.

https://www.hipaajournal.com/march-2019-healthcare-data-breach-report/

https://www.gartner.com/smarterwithgartner/navigating-the-security-landscape-in-the-iot-era/
[36] Zhaohao Sun, Kenneth David Strang & Francisca Pambel “Privacy and Security in the Big Data Paradigm” Journal Computer Information Systems, Volume 60, 2020 - Issue 2, Pages 146-155, 2018 https://doi.org/10.1080/08874417.2017.1418631

[37] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, “Twenty security considerations for cloud-supported internet of Journal of Computer Networks and Communications 11 things,” IEEE Internet of Things Journal, vol. 3, no. 3, pp. 269–284, 2016.

[38] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, “Twenty security considerations for cloud-supported internet of Journal of Computer Networks and Communications 11 things,” IEEE Internet of Things Journal, vol. 3, no. 3, pp. 269–284, 2016.

[39] A. K. Das, S. Zeadally, and D. He, “Taxonomy and analysis of security protocols for internet of things,” Future Generation Computer Systems, vol. 89, pp. 110–125, 2018.

[40] Y. Yang, H. Peng, L. Li, and X. Niu, “General theory of security and a study in internet of things,” IEEE Internet of Things Journal, vol. 4, no. 2, pp. 592–600, 2017.

[41] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, “Internet of Things for healthcare: a comprehensive survey,” IEEE Access, vol. 3, pp. 678–708, 2015.

[42] Aufner, P., “The IoT security gap: a look down into the valley between threat models and their implementation,” International Journal Information Security, 19, 3–14 2020.

[43] https://doi.org/10.1007/s10207-019-00445-y

[44] Gaur, M. S., Pant, B. “Trusted and secure clustering in mobile pervasive environment”, Human-Centric Computer Information Sciences 5, 32 (2015). https://doi.org/10.1186/s13673-015-0050-1

[45] Madhu Sharma Gaur, Bhaskar Pant, “Impact of Signal-Strength on Trusted and Secure Clustering in Mobile Pervasive Environment”, Procedia Computer Science, Volume 57, 2015, Pages 178-188, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2015.07.418. http://www.sciencedirect.com/science/article/pii/S187705091501947X

[46] F. Brasser, B. El Mahjoub, A.-R. Sadeghi, C. Wachsmann, and P. Koeberl, “TyTAN: Tiny Trust Anchor for Tiny Devices,” in Proceeding 52nd ACM/EDAC/IEEE Design Automation Conference (DAC ’15), pp. 1–6, San Francisco, CA, USA, June 2015.

[47] B. Pourghebleh, K. Wakil, and N. J. Navimipour, “A comprehensive study on the trust management techniques in the Internet of Things,” IEEE Internet Things J., vol. 6, no. 6, pp. 9326–9337, 2019.