Mediterranean Smart Cities Conference (MSCC 2024)
2-4 May, 2024, Martil, Morocco

Multi parameter Multilevel (MPML) Based Trust Management System for Healthcare

Mrs. Bhawana Ahire
Ph.D. Scholar, Department of
Computer Engineering
SKNCOE, Pune, India
bhawanasragvi@gmail.com

Dr. Sachin Sakhare
Professor & Head, Department of
Computer Engineering, BRACT's Vishwakarma
Institute of Technology, Pune, India
sachin.sakhare@viit.ac.in

Abstract— **Resounding extension of the Internet of Things (IoT) has garnered substantial attention from the scientific community over the last two decades. The infusion of IoT has intricately connected our world, endowing intelligent devices with the finesse to adeptly perform daily tasks. Swift technological progress in this arena foreshadows the continued evolution of diverse smart applications, ranging from intelligent healthcare and homes to futuristic cities. Nevertheless, the surge in interconnected nodes within the expansive IoT network brings forth a formidable scalability concern, given the heterogeneity of these nodes in terms of processing power, energy consumption, and capacity.**

Conventional security measures, while crucial, fall short in effectively safeguarding these intricate smart applications. Addressing this exigency, the role of trust becomes paramount in mitigating the vulnerabilities that arise when IoT nodes interlink with the digital realm. Amidst this backdrop, diverse trust models, spanning direct, indirect, and hybrid trust computation methods, have been proposed for trust management. However, these models often grapple with adapting comprehensively to the dynamic and ever-evolving nature of intelligent IoT systems. In response, the proposed system introduces a sophisticated three-tiered approach: Trust Calculation, Propagation, and modification. Centerpiece of the system is a meticulously crafted trust calculation algorithm, bespoke for IoT devices. This algorithm harmoniously integrates considerations of both direct and indirect trust, underpinned by a multi-parameter multilevel trust calculation framework. The overarching aim is to attain the pinnacle of precision in evaluating the trustworthiness intrinsic to this intricate IoT landscape.

Keywords— Trust management; Trust computation algorithm; Healthcare monitoring; Machine learning-driven approach

I. Introduction

While the Internet of Things offers substantial benefits to the world, it also presents a range of challenges for authors and programmers. One of the primary difficulties is the heterogeneity of IoT devices, which vary in physical attributes such as sensors, actuators, processing power, battery capacity, and operating systems [1]. With the projected exponential growth of connected devices within the IoT network over the next decade, the importance of scalability and cost considerations will magnify significantly. To avoid potential bottlenecks, adopting a decentralized approach for IoT proves advantageous [2]. However, addressing several critical security concerns is imperative. These include authentication, key management, access control, availability, safety, trust management, and coping with the resource limitations in IoT applications. Successfully overcoming these security challenges is essential for ensuring the continued growth and success of the Internet of Things in enhancing various aspects of our lives.

The Internet of Things (IoT) is ushering in a groundbreaking revolution in the contemporary world, where everyday devices in our environment are becoming intelligent and capable of performing tasks with greater precision[3]. The IoT architecture is diverse, granting nodes autonomy to communicate and share information with other nodes seamlessly. The integration of IoT and healthcare has led to remarkable advancements in patient monitoring and care. Nevertheless, a significant challenge lies in detecting and addressing malicious and compromised nodes, which poses a critical concern for the reliability of IoT systems in healthcare and security.

Within the realm of healthcare, patient tracking and monitoring hold immense potential to revolutionize the industry. The utilization of injectable, wearable, and implantable IoT systems enables the collection of vital data, such as pulse and heart rate, blood pressure, directly from patients [4]. With an abundance of information available, medical diagnoses and subsequent treatments can become significantly more accurate. This data not only provides insights into underlying symptoms but also facilitates remote health monitoring and diagnosis, ensuring comprehensive care [5].

These IoT applications are particularly critical for elderly individuals and those living alone, where continuous monitoring can offer vital support and prompt medical attention when needed[6]. However, to ensure the effectiveness and safety of such healthcare IoT systems, it is crucial to establish trustworthy communication between the diverse and scalable devices involved in the process[7]. Through tackling these obstacles, IoT technologies have the potential to assume a crucial role in elevating healthcare quality and enriching the well-being of patients [8].Hence, the present paper puts forward a Trust Management System tailored for the realm of Healthcare IoT.

The following segments of this paper are organized as follows: Section 2 delves into an extensive examination of the pertinent literature on the Trust Management System in Healthcare IoT. In Section 3, we introduce our Proposed System, elaborating on its structure and operational mechanisms. The Results and Discussion are encompassed in Section 4, wherein we showcase and dissect the results achieved by our proposed system. Ultimately, Section 5 encapsulates our concluding remarks, succinctly summarizing the principal discoveries and ramifications of our investigation.

II. Related Work

Alemdar et al.[9] introduced an IoT-based universal healthcare system that integrates a wireless sensor network (WSN) architecture in an energy-efficient manner, focusing on the IoT paradigm. The concept of trust holds significant importance within the realm of IoT devices, particularly within Health IoT systems. This article presents an innovative Healthcare IoT system model that offers real-time updates on patients' current health statuses [10]. Leveraging Raspberry Pi 3 technology, the system facilitates prompt responses by providing patients with information about nearby hospitals and physician availability.

S. Yattinahalli et al. [13] presents a solution for patients who find themselves in unfavorable locations due to unavoidable circumstances, despite being aware of the poor conditions that may not be suitable for their health. The technology incorporated in the proposed system helps such patients navigate through challenging situations, ensuring they receive timely assistance and support, ultimately safeguarding their health and well-being[11]. Binomial Distribution-based Trust Management Scheme for Healthcare IoT deals with on-off attacks as well as Bad mouthing attacks [14]. Weizhi Meng et al. developed a Bayesian-Based Trust Management technique to deal with insider attacks and identify malicious devices in the healthcare environment [15]. However, the proposed system lacks scalability as well as detection sensitivity that needs to be improved.

Drawing upon our research findings, Shariq Aziz Butt et al. proposed suggestive measures to mitigate these attacks, ensuring the robustness and security of health monitoring systems. By addressing these critical issues, they enhance the reliability and effectiveness of such systems, ultimately benefiting patients and healthcare providers alike [16]. In the year 2020, Behshid Shayesteh et al. introduced a hybrid trust management scheme tailored for IoT-enabled health monitoring systems [17]. In this study, they put forth a Bayesian learning-based procedure aimed at estimating the entities (trust score of users). This procedure proves highly effective in discerning the behavioral inclinations of users concerning the accuracy of their reported observations. By employing this approach, it can accurately assess the reliability and credibility of user-contributed data, enhancing the overall trustworthiness and quality of the system's output. However, this system needs to be implemented in the real-world environment and validated. Heterogeneity and scalability need to be dealt with [18].

Anis Tissaoui et al. conducted a comprehensive investigation into the challenges and opportunities presented by IoT in the realm of smart healthcare, as documented in their study in 2020 [19]. The research aims to analyze the factors influencing uncertainty and ambiguity in IoT-based healthcare systems, specifically focusing on their development within the healthcare industry. Furthermore, the study offers valuable recommendations for guiding future research directions, seeking to address these challenges and capitalize on the opportunities to advance smart healthcare technologies. In their work, H.A. El Zouka et al. [20] present a secure and lightweight authentication scheme with the primary objective of protecting personal health information and establishing secure communication channels. The scheme offers robust protection, ensuring the confidentiality and integrity of sensitive healthcare data, thereby instilling trust and confidence in the system's overall security measures.

Abdul Rauf et al. [21] designed a mathematical miniature to calculate trust between devices for healthcare applications. The aforementioned system's primary focus is not on achieving pinpoint accuracy and efficiency alone; rather, it necessitates practical implementation within a real-world context, facilitated through the utilization of Raspberry Pi. In today's dynamic landscape, the Social Internet of Things (SIoT) has captivated the scientific realm owing to its emphasis on fostering social connectivity among proximate entities. Expanding on this, Mohammed Rizwanullah et al. [22] put forward an innovative trust management model tailored for SIoT. This model hinges on the utilization of multi-criteria decision-making, while trust calculation is ingeniously underpinned by a fuzzy-based methodology. It's pertinent to note, however, that the efficacy of the proposed model shines in scenarios encompassing relatively modest datasets and a confined array of trust metrics. Navigating the challenges posed by voluminous data streams and the ever-evolving behavior of IoT devices, Yara Alghofaili et al. [23] introduce a pioneering approach to detecting trust-related attacks in IoT devices. Their model ingeniously relies on the Long Short-Term Memory (LSTM) technique, thereby adeptly accommodating the intricacies of abundant data and the dynamic nature of IoT environments.

In an extensive investigation, A. Rejeb et al. [24] meticulously analyzed a comprehensive compilation of 2990 journals, with a specific focus on exploring the diverse applications of IoT within the healthcare sector. Their findings culminated in the discernment that block chain technology emerges as a particularly promising avenue, effectively bolstering the implementation of IoT in healthcare. This technological synergy is pivotal in ensuring a myriad of benefits, including but not limited to enhanced transparency, fortified security for patient data, streamlined drug traceability, and heightened efficiency in data sharing. Considering trust in healthcare applications, S. R. Joshua et al. [25] proposed a 2 Diabetic Mellitus Mobile Application. The proposed system successfully monitors patients' details such as Medication, Food Intake, Exercise, Sleep, etc. The proposed app can be integrated with a Smart plate so that patients with Diabetes can control their activity, health through diet, and meditation. In summary, addressing the issue of trust management is a pivotal concern, particularly when it comes to IoT devices and services. The existing body of literature has put forth various potential remedies, as explored in the preceding discussion. Nevertheless, certain substantial research voids persist, and these are encapsulated in the subsequent sections.

III. Proposed System

Amidst the ongoing COVID scenario, wireless health monitoring has emerged as a paramount concern for nations worldwide, affecting hospitals and various healthcare centers. Data from diverse sensors such as temperature sensors, pulse ox meters, and blood pressure sensors appears accurate yet it remains vulnerable to potential attacks either during its origination or while traversing the transmission path. Moreover, a looming threat exists in the form of intentional manipulation by malicious software, posing a security breach via the Internet. This distorted data, if left unchecked, could significantly impact critical life-or-death decisions. This raises a crucial question: how can we instill trust in the accuracy of information provided by an IoT-powered healthcare framework?

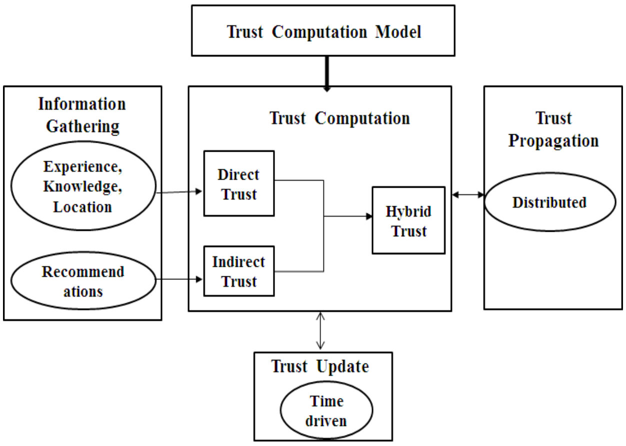


Figure 1. Trust Management System

As the IoT becomes an integral part of the healthcare landscape, nurses find themselves tasked with mastering a range of technologies to optimize patient outcomes. A similar adaptability to technology is expected from other healthcare practitioners as well. Trust encompasses various dimensions, spanning multiple domains. According to Cook's analysis [28], trust entails a subjective confidence in the actions of a particular entity. The process of formulating and implementing strategies to measure and maintain trust in diverse entities or systems is referred to as Trust Management (TM) [29]. As depicted in Figure 3, a tangible visual representation of the Trust Management (TM) system unfolds, delineating its constituent phases in a coherent manner.

A. *Information Gathering*

Prior to the conception of any Trust Management (TM) System, a fundamental preliminary stride involves the meticulous curation of input parameters earmarked for the computation of trust values [30]. The proposed system is built upon multi-parameter and multilevel attributes. It distinguishes professional, personal, and demographic information as direct attributes, while considering Social information, such as the number of followers, as an indirect attribute.

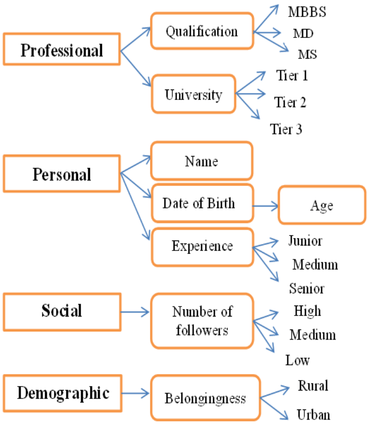


Figure 2. Information Gathering

Personal information includes details such as the Name of the professional and date of birth, which further allows derivation of the Age and Experience. Experience is categorized into Junior (less than 5 years), Medium (between 5-10 years), and Senior (more than 10 years). Professional information encompasses the Educational Qualification, where MBBS is categorized as level 1, MD as level 2, and MS as level 3. The qualifications are obtained from Universities, with Tier 1 (Government) colleges classified as level 1, Tier 2 colleges as level 2, and Tier 3 colleges as level 3.

B. *Trust Computation*

This phase focuses on trust computation using the data collected during Phase 1, which is the Information Gathering phase. Once data is collected and organized into levels, a trust computation model is applied based on indirect and direct trust. Various authors have employed different models for this purpose, including Fuzzy Logic, Machine Learning, Bayesian Distribution, Block chain-based, and Hybrid models. The trust computation algorithm is designed as follows:

Algorithm: For calculating trust of the node

```
Input: Weights for direct and indirect trust α and β
Output: Final trust value $T_i^f$
1.  $T_i^d$ ← Direct trust ($P_i$)
2.  $T_i^R$ ← Indirect trust (i)
3.  Calculate First Direct Trust using Eq. 1
4.  Calculate Indirect Trust using Eq. 2
5.  Calculate Final i.e. Hybrid Trust using Eq. 3
```

Direct trust calculation:

$$T_i^d = a * b^x + c * d^x + e * f^x \text{-----------Eq. (1)}$$

Indirect trust calculation:

$$\sum_{i\,j}^{n} = \frac{1}{n} T_{i\,j}^{R}$$ --------------------------------------Eq. (2)

Final trust calculation:

$$T_i^f = \alpha * T_i^d + \beta * T_i^R$$ ---------------------Eq. (3)

In the calculation of direct trust, factors like Experience, Knowledge, and Location are considered. For Indirect trust calculation, Recommendations are taken into account. Once information is gathered in Phase 1, equal weights are assigned to each attribute. Subsequently, Direct and Indirect trust are calculated simultaneously using Equations 1 and 2. The calculation of Hybrid trust is then performed using Equation 3.

Given the larger sample size, a machine learning approach is employed. The proposed system, based on multiple attributes and multilevel criteria selection, contributes to enhanced accuracy.

C. *Trust Propagation*

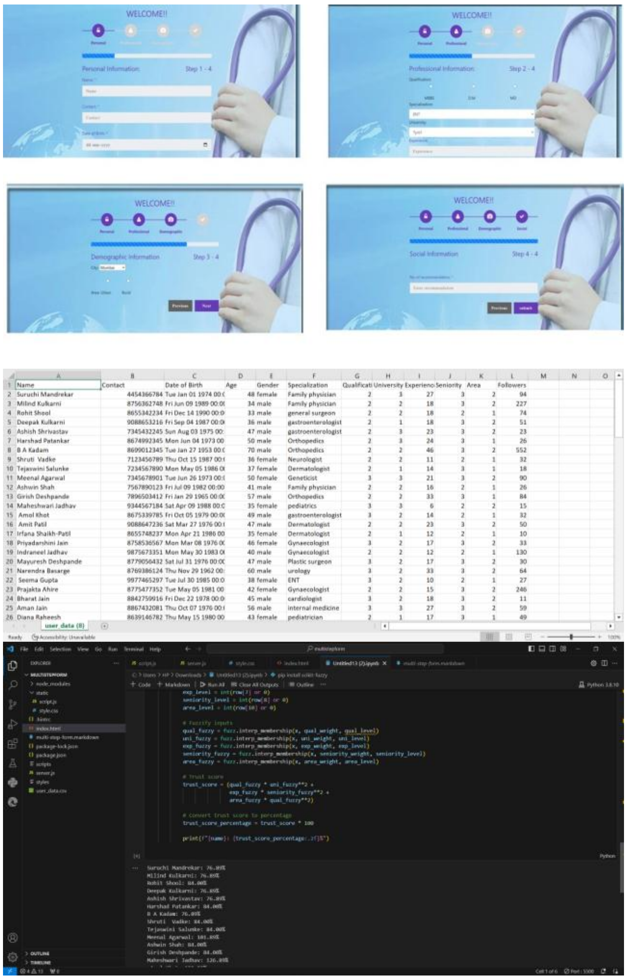
Once trust is calculated in Phase 2, it must be propagated to neighboring nodes according to the chosen architecture (Centralized, Distributed, Semi-distributed). In the distributed approach, each node contributes to collecting information, trust computation, and updating.

D. *Trust Update*

After trust is propagated, the trust values need to be updated. The computed trust score can be updated either through time-driven (at regular time intervals) or event-driven (triggered by specific events) approaches. The proposed system utilizes a time-driven approach, updating the trust values every 2 seconds. This frequency ensures more accurate results, which is crucial in healthcare applications where timely diagnosis is essential. The proposed system's accuracy is enhanced due to the larger dataset resulting from the continuous readings obtained every 2 seconds.

IV. Results and Discussion

We have developed a Privacy-aware Health Access Control System with a focus on privacy concerns, addressing encryption vulnerabilities, and preventing the exposure of confidential healthcare data. Our system operates across four distinct phases: Information Gathering, Trust Computation, Trust Propagation, and Trust Update. The subsequent screenshots provide a visual representation of these phases. Direct information such as Personal, Professional, Demographic Information is considered whereas, number of followers (i.e. Recommendations) as indirect. Fig. 3 denotes screenshots of such information gathering.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Name	Contact	Date of Birth	Age	Gender	Specialization	Qualificati	University	Experieno	Seniority	Area	Followers			
2	Suruchi Mandrekar	4454366784	Tue Jan 01 1974 00:0	48	female	Family physician	2	3	27	3	2	94			
3	Milind Kulkarni	8756362748	Fri Jun 09 1989 00:0	34	male	Family physician	2	2	18	3	2	227			
4	Rohit Shool	8655342234	Fri Dec 14 1990 00:0	33	male	general surgeon	2	2	18	2	1	74			
5	Deepak Kulkarni	9088653216	Fri Sep 04 1987 00:0	36	male	gastroenterologist	2	1	18	3	2	51			
6	Ashish Shrivastav	7345432245	Sun Aug 03 1975 00:	47	male	gastroenterologist	2	3	23	3	2	23			
7	Harshad Patankar	8674992345	Mon Jun 04 1973 00	50	male	Orthopedics	2	3	24	3	1	26			
8	B A Kadam	8699012345	Tue Jan 27 1953 00:0	70	male	Orthopedics	2	2	46	3	2	552			
9	Shruti Vadke	7123456789	Thu Oct 15 1987 00:0	36	female	Neurologist	2	2	11	2	1	32			
10	Tejaswini Salunke	7234567890	Mon May 05 1986 0	37	female	Dermatologist	2	1	14	3	1	18			
11	Meenal Agarwal	7345678901	Tue Jun 26 1973 00:0	50	female	Geneticist	3	3	21	3	2	90			
12	Ashwin Shah	7567890123	Fri Jul 09 1982 00:00	41	male	Family physician	2	2	16	2	1	26			
13	Girish Deshpande	7896503412	Fri Jan 29 1965 00:0	57	male	Orthopedics	2	2	33	3	1	84			
14	Maheshwari Jadhav	9344567184	Sat Apr 09 1988 00:0	35	female	pediatrics	3	3	6	2	2	15			
15	Amol Khot	8675339785	Fri Oct 05 1979 00:0	49	male	gastroenterologist	3	2	14	2	1	32			
16	Amit Patil	9088647236	Sat Mar 27 1976 00:0	47	male	Dermatologist	2	2	23	3	2	50			
17	Irfana Shaikh-Patil	8655748237	Mon Apr 21 1986 00	35	female	Dermatologist	2	1	12	2	1	10			
18	Priyadarshini Jain	8758536567	Mon Mar 08 1976 00	46	female	Gynaecologist	3	2	17	3	2	33			
19	Indraneel Jadhav	9875673351	Mon May 30 1983 0	40	male	Gynaecologist	2	2	12	2	1	130			
20	Mayuresh Deshpande	8779050432	Sat Jul 31 1976 00:00	47	male	Plastic surgeon	3	2	17	3	2	30			
21	Narendra Basarge	8769386124	Thu Nov 29 1962 00:	60	male	urology	3	2	33	3	2	64			
22	Seema Gupta	9977465297	Tue Jul 30 1985 00:0	38	female	ENT	3	2	10	2	1	27			
23	Prajakta Ahire	8775477352	Tue May 05 1981 00	42	female	Gynaecologist	2	2	15	3	2	246			
24	Bharat Jain	8842759916	Fri Dec 22 1978 00:0	45	male	cardiologist	3	2	18	3	2	11			
25	Aman Jain	8867432081	Thu Oct 07 1976 00:0	56	male	internal medicine	3	3	27	3	2	59			
26	Diana Raheesh	8639146782	Thu May 15 1980 00	43	female	pediatrician	2	1	17	3	1	49			

```
        exp_level = int(row[7] or 0)
        seniority_level = int(row[8] or 0)
        area_level = int(row[10] or 0)

        # Fuzzify inputs
        qual_fuzzy = fuzz.interp_membership(x, qual_weight, qual_level)
        uni_fuzzy = fuzz.interp_membership(x, uni_weight, uni_level)
        exp_fuzzy = fuzz.interp_membership(x, exp_weight, exp_level)
        seniority_fuzzy = fuzz.interp_membership(x, seniority_weight, seniority_level)
        area_fuzzy = fuzz.interp_membership(x, area_weight, area_level)

        # Trust score
        trust_score = (qual_fuzzy * uni_fuzzy**2 +
                       exp_fuzzy * seniority_fuzzy**2 +
                       area_fuzzy * qual_fuzzy**2)

        # Convert trust score to percentage
        trust_score_percentage = trust_score * 100

        print(f"{name}: {trust_score_percentage:.2f}%")
```

```
Suruchi Mandrekar: 76.89%
Milind Kulkarni: 76.89%
Rohit Shool: 84.00%
Deepak Kulkarni: 76.89%
Ashish Shrivastav: 76.89%
Harshad Patankar: 84.00%
B A Kadam: 76.89%
Shruti  Vadke: 84.00%
Tejaswini Salunke: 84.00%
Meenal Agarwal: 101.89%
Ashwin Shah: 84.00%
Girish Deshpande: 84.00%
Maheshwari Jadhav: 126.89%
```

Figure 3. Screenshots of Trust Management System Calculation

We have compared our proposed Multi Parameter Multi-Level(MPML) based trust management system for healthcare with existing systems. Fig. 4 shows graphical analysis for the same.

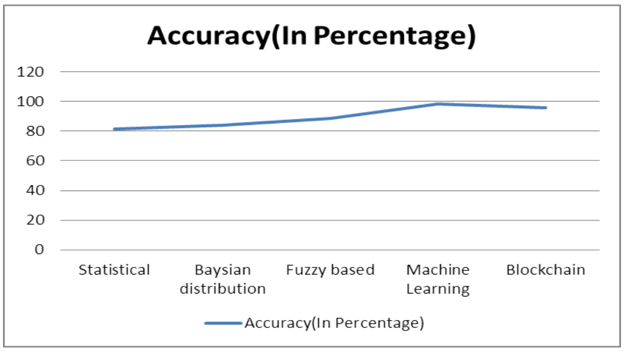


Figure 4. Graphical Analysis of different Trust Management System

V. Conclusion

The Internet of Things (IoT) is swiftly revolutionizing contemporary living by infusing everyday devices with unparalleled intelligence, empowering them to accomplish tasks with remarkable accuracy. This convergence of IoT with healthcare holds immense potential, particularly in patient monitoring. Yet, a considerable obstacle persists in detecting compromised nodes or malicious intent within the IoT ecosystem. This article introduces an innovative machine learning-driven approach to trust management, intricately incorporating both direct and indirect trust components.

Our proposed methodology hinges on the amalgamation of knowledge and experience facets of trust, intricately derived from diverse parameters. This framework is founded on a multi-parameter, multi-level attribute trust calculation, which significantly augments precision. Remarkably, when juxtaposed with existing machine learning techniques, our model demonstrates unparalleled proficiency in mitigating trust-related challenges inherent to the realm of IoT.

REFERENCES

[1] Xu, L. D. (1999). Internet of Things (IoT): An Introduction. Wiley Encyclopedia of Electrical and Electronics Engineering, 1-10.

[2] Cohen, J. E. (2003). Human population: The next half century. Science, 302(5648), 1172-1175.

[3] Khanna, A., & Kaur, S. (2020). Internet of Things (IoT), applications and challenges: A comprehensive review. Wireless Personal Communications, 114, 1687-1762.

[4] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer Networks, 54, 2787-2805.

[5] Putra, G. D., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2019). Trust management in decentralized IoT access control system. arXiv preprint arXiv:1912.10247.

[6] Mendoza, C. V., & Kleinschmidt, J. H. (2015). Mitigating on-off attacks in the internet of things using a distributed trust management scheme. International Journal of Distributed Sensor Networks, 11(11), 859731.

[7] Meena Kowshalya, A., & Valarmathi, M. L. (2017). Trust management for reliable decision making among social objects in the social internet of things. IET Networks, 6(4), 75-80.

[8] Mahalle, P. N., Thakre, P. A., Prasad, N. R., & Prasad, R. (2013). A fuzzy approach to trust-based access control in internet of things. In Wireless VITAE (pp. 1-5).

[9] Alemdar, H., & Ersoy, C. (2010). Wireless sensor networks for healthcare: A survey. Computer Networks, 54(15), 2688-2710.

[10] Pang, Z. (2013). Technologies and architectures of the Internet-of-Things (IoT) for health and well-being (Master's thesis, KTH-Royal Institute of Technology).

[11] Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: A comprehensive survey. IEEE Access, 3, 678-708.

[12] Alamelu, J. V., & Mythili, A. (2017). Design of IoT based generic health care system. In 2017 International Conference on Microelectronic Devices, Circuits and Systems (ICMDCS) (pp. 1-4).

[13] Yattinahalli, S., & Savithramma, R. M. (2018). A Personal Healthcare IoT System model using Raspberry Pi 3. 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), (pp. 569-573).

[14] Fang, W., Zhu, C., Chen, W., Zhang, W., & Rodrigues, J. J. P. C. (2018). BDTMS: Binomial Distribution-based Trust Management Scheme for Healthcare-oriented Wireless Sensor Network. 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), (pp. 382-387).

[15] Meng, W., Choo, K. K. R., Furnell, S., Vasilakos, A. V., & Probst, C. W. (2018). Towards Bayesian-Based Trust Management for Insider Attacks in Healthcare Software-Defined Networks. IEEE Transactions on Network and Service Management, 15(2), 761-773.

[16] Butt, S. A., Diaz-Martinez, J. L., Jamal, T., Ali, A., De-La-Hoz-Franco, E., & Shoaib, M. (2019). IoT Smart Health Security Threats. 2019 19th International Conference on Computational Science and Its Applications (ICCSA), (pp. 26-31).

[17] Shayesteh, B., Hakami, V., & Akbari, A. (2020). A trust management scheme for IoT-enabled environmental health/accessibility monitoring services. International Journal of Information Security, 19, 93-110.

[18] Alraja, M. N., Farooque, M. M. J., & Khashab, B. (2019). The Effect of Security, Privacy, Familiarity, and Trust on Users' Attitudes Toward the Use of the IoT-Based Healthcare: The Mediation Role of Risk Perception. IEEE Access, 7, 111341-111354.

[19] Tissaoui, A., & Saidi, M. (2020). Uncertainty in IoT for Smart Healthcare: Challenges, and Opportunities. In The Impact of Digital Technologies on Public Health in Developed and Developing Countries (pp. 1-19). Springer.

[20] El Zouka, H. A., & Hosni, M. M. (2021). Secure IoT communications for smart healthcare monitoring system. Internet of Things, 13, 100036.

[21] Rauf, A., Shaikh, R. A., & Shah, A. (2022). Trust Modeling and management for IoT healthcare. International Journal of Microwaves and Wireless Technologies, 12, 21-35.

[22] Rizwanullah, M., Ahmed, I., & Imran, M. (2022). Development of a Model for Trust Management in the Social Internet of Things. Electronics, 12(1), 41.

[23] Alghofaili, Y., & Rassam, M. A. (2023). A Dynamic Trust-Related Attack Detection Model for IoT Devices and Services Based on the Deep Long Short-Term Memory Technique. Sensors, 23(8), 3814.

[24] Rejeb, A., Ghedira, G., & Zemmari, N. (2023). The Internet of Things (IoT) in healthcare: Taking stock and moving forward. Internet of Things, 100721.

[25] Joshua, S. R., Kishore, M. R., & Ghanakrishnan, S. (2023). Trust Components: An Analysis in The Development of Type 2 Diabetic Mellitus Mobile Application. Applied Sciences, 13(3), 1251.

[26] Veith, B., Krummacker, D., & Schotten, H. D. (2023). The road to trustworthy 6G: A survey on trust anchor technologies. IEEE Open Journal of the Communications Society, 4, 581-595.

[27] Dhagarra, D., Goswami, M., & Kumar, G. (2020). Impact of trust and privacy concerns on technology acceptance in healthcare: An Indian perspective. International Journal of Medical Informatics, 141, 104164.

[28] Cook, K. (2001). Trust in Society. Russell Sage Foundation.

[29] Din, I. U., Guizani, M., Kim, B. S., Hassan, S., & Khan, M. K. (2018). Trust Management Techniques for the Internet of Things: A Survey. IEEE Access, 7, 29763-29787.

[30] Pourghebleh, B., & Navimipour, N. J. (2017). Data aggregation mechanisms in the Internet of things: A systematic review of the literature and recommendations for future research. Journal of Network and Computer Applications, 97, 23-34.

[31] Yue, Y., Li, S., Legg, P., & Li, F. (2021). Deep Learning-Based Security Behaviour Analysis in IoT Environments: A Survey. Security and Communication Networks, 2021, 8873195.

[32] Anagnostopoulos, M., Spathoulas, G., Viaño, B., & Augusto-Gonzalez, J. (2020). Tracing Your Smart-Home Devices Conversations: A Real World IoT Traffic Data-Set. Sensors, 20, 6600.

[33] Crawford, M., Khoshgoftaar, T. M., Prusa, J. D., Richter, A. N., & Al Najada, H. (2015). Survey of review spam detection using machine learning techniques. Journal of Big Data, 2, 23.

[34] Sugeng, W., Istiyanto, J. E., Mustofa, K., & Ashari, A. (2015). The impact of QoS changes towards network performance. International Journal of Computer Networks & Communications, 3, 48-53.

[35] Zach. (2021). Normalization in Statology. Statology.