Towards Robust Ubicomp: A Comprehensive Review on the Grand Challenges of Ubiquitous Computing

G.W.Y.S. Boralessa[1], K.W.A.H. Samarasinghe[2], T.N. Ahamed[3] & A.R.F. Shafana[4*]

[1,2,3,4]*Department of Information and Communication Technology, Faculty of Technology, South Eastern University of Sri Lanka, Sri Lanka*

[1]*geethyapa@gmail.com,* [2]*achisamareee@gmail.com,* [3]*nuskyahamed18@gmail.com,* [4*]*arfshafana@seu.ac.lk*

Abstract- *Ubiquitous Computing is a concept that consists of qualities that enable people to move away from traditional desktop computing systems and toward computer systems, where everything is available and accessible everywhere through various devices while being essentially invisible. The purpose of this paper is to provide a comprehensive review of the literature on the challenges of ubiquitous computing with the objective of synthesizing existing knowledge and offering direction for future research. Furthermore, systematic reviews of challenges that obstruct ubiquitous computing's success are scarce. Therefore, this paper carefully reviewed a number of published papers based on their contributions to the body of knowledge in ubiquitous computing and has identified six grand challenges that are critical to the future of ubiquitous computing. Such as social, legal, and ethical Issues, technical issues, architectural issues, human and environmental challenges, security challenges and system maintenance challenges. Since the empirical study, development, and validation of Ubicomp systems are still in their early stages, this may deter practitioners from using solutions from the literature. In that ground, our findings would enable academics and practitioners to construct robust Ubicomp systems with the knowledge transfer from this study. Since our study consolidates the vulnerable challenges in one place, the findings of the study could be readily adapted to overcome challenges when building ubiquitous systems and services.*

Keywords: Ubiquitous Computing, Societal Issue, Ubiquitous Manufacturing, Pervasive, Ubicomp

I. INTRODUCTION

Knowledge has become immediate, automatic, and pervasive as everyone can now view information everywhere, at any moment, and in a customized manner due to the advanced technology such as the miniaturization of microprocessors and sensors in combination with the proliferation in networking technology. The trend in recent years, with both the development of digital data and information technologies, has been to outsource data collection and processing to cloud-based platforms, which now shapes the architectures of ubiquitous computing and connectivity (Qiu *et al.*, 2019). Ubiquitous computing is an emerging technology in computer science (Mirani *et al.*, 2017). The most significant technologies are those that vanish, and they blend into the fabric of ordinary life until they are undetectable (Weiser, 1999) thus commenced the vision of ubiquitous computing, often known as pervasive computing.

The aim of ubiquitous computing is to make machines available in a nonintrusive manner in the physical world, making them almost, if not completely, invisible to the user (Weiser, 1993). Also as a basic necessity of time, technology is swiftly finding its approach and changing states quicker than speed into every part of our existence. Since the pervasive environment allows communication between devices at any time and from any location, systems are becoming more pervasive in the modern world (Shaheed *et al.*, 2015). Overall ubiquitous computing infrastructure offers a network that can combine various computation tools in software and hardware while offering a pay for use service for end users.

Applications of ubiquitous computing are widespread across Retail, Industrial production and material management, Transport logistics, Personal identification and authentication, Health care and Mobility and transport (Friedewald and Raabe, 2011). Also there are many applications derived from each respective path. However, as the number of individuals using ubiquitous computing grows, the problems also arise. Further, there is a trend toward ubiquitous computing, which refers to the use, development, encoding, dissemination, and storing of information in a way that is both transparent and invisible. Everyday objects are evolving into smart objects that are networked, respond to their

surroundings, and communicate with their users (Sen, 2010). This is a major influence for the difficulties which occur with ubiquitous computing. In the perspective of the process, smart and intelligent, embedded or stand-alone ubiquitous computing environments are seen as vastly different from conventional desktop computing environments in terms of design, creation, and execution. Actually, these have proved to be difficult challenges, necessitating the consideration of many technical, societal, operational, and environmental factors (Horváth and Vroom, 2015).

As ubiquitous computing and its associated challenges are at a rapidly increasing pace, this demands a critical analysis of the challenges encountered to propose a mechanism and a framework to overcome these challenges. Therefore, this study aims to analyze a compendium of literature in the domain of ubiquitous computing and identify the most critical challenges of ubiquitous computing. The outcome of this research can be utilized by ubiquitous computing service providers and application developers to mitigate it during the development process.

Despite the rapid advancement of information and networking technologies, which has resulted in the existence of ubiquitous computing, there are still many legal, ethical, and technological barriers that preclude society from reaping the benefits of such advancement (Mahmoud, 2016). Thus, this work is important to obtain the potential benefit of ubiquitous computing in its fullest form while mitigating the challenges. The rest of the paper is organized as follows. Review of challenges in ubiquitous computing are identified and described respectively. Afterwards the findings from the review are discussed to provide research perspectives followed by the conclusion of our study.

II. RELATED WORKS

Iwaya, Ahmad and Ali Babar (2020) undertook a systematic mapping study on mobile health and ubiquitous health systems with special attention to privacy and security concerns. The study was able to systematically analyze state-of-the-art literature on the relevant field and listed potential challenges encountered in the specific field. The researchers suggested that many of the challenges in ubiquitous health systems are still under-represented and provided a list of challenges in the field. However, this work is confined to ubiquitous health systems and our study focuses on the ubiquitous systems as a whole.

The research of Mirani *et al.* (2017) is quite significant for its contribution in identifying the applications, challenges and the elements of ubiquitous computing. However, the study was pivoted around the challenges relevant to the performance of ubiquitous computing in contrast to our work that combines many challenges around. Another comprehensive survey analyzed the challenges of ubiquitous computing with special reference to location based services alone (Jiang *et al.*, 2021). Comprehensive surveys in ubiquitous computing and Internet of Things by Hashemi and Zarei (2021) identified resource management and security issues as challenges while security issues were spotted as major challenge in the works of Adat and Gupta, (2018); Burhan *et al.*, (2018); and Malhotra *et al.*, (2021).

Many systematic studies have been undertaken to identify the potential challenges in the domain of ubiquitous computing. However, the challenges are widespread across several literature that does not allow the practitioners to readily identify all the prominent challenges and adopt the measures when employing ubiquitous systems. Thus, this secondary study facilitates the interested group with the consolidated knowledge and evidence with easy access.

III. METHODOLOGY

Systematic approach has been employed to undertake our study to achieve its objectives. An in-depth investigation of various learning techniques has been used to protect the Ubicomp system in one way or another. This review was conducted using related research publications in the field of ubiquitous computing. The methodology adopted is presented in Figure 01.

The focus of this research is to investigate the available literature in order to gain a better knowledge and insight into recent developments and challenges in the ubicomp field. This technique lays out the fundamental procedures for locating, comprehending, and analyzing research publications, which would help to identify supporting evidence easier. A proper professional planning and validation of search strings was carried out as part of the search plan. The research articles are mainly from Scopus database that are recent and with high citations. Scopus was chosen

as it is a comprehensive source of research articles. From the search results, the peer-reviewed and high-quality database journals and reputed conferences like IEEEXplore, Springer, Wiley, ACM, Elsevier, and Google Scholar were filtered to investigate the challenges in ubiquitous computing.

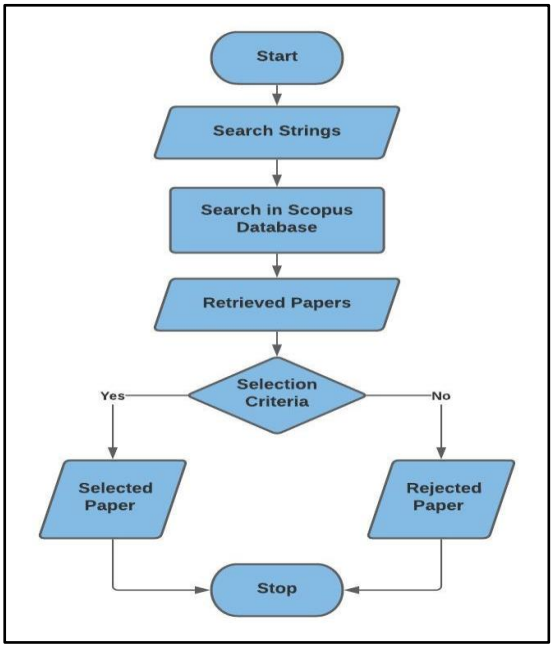

Figure 01: Adopted Methodology

The search phrases were carefully crafted in response to the research question. The search keywords were adjusted several times in order to assemble practically all of the relevant papers. As a result, several search strings with different combinations of words were utilized to find relevant papers. "Ubiquitous Computing" AND "Challenges" AND "Social, Legal, and Ethical Issues" OR "Technical Issues" OR "Architectural Issues" OR "Human and Environmental Challenges" OR "Security Challenges" OR "System Maintenance Challenges". An automated search was conducted using these search strings using the search engines of numerous digital libraries. The paper selection criteria were then used to further filter out the most relevant research in this field. The rest of the paper discusses the grand challenges of Ubicomp which we derived from the review.

IV. GRAND CHALLENGES IDENTIFIED

A. Security Challenges

Security has been identified as one of the major challenges in ubiquitous computing over the past studies. This becomes a serious challenge since people never liked to disclose their personal, sensitive, and mission-critical information over a model or in ubicomp as they consider that is not safe or not considered to be secure. In a ubiquitous computing environment, eavesdropping on communication media, denial of service (DOS), and data manipulation are examples of hackers' attack getting control of user instruments or devices (Sharifi, Khosravi and Shah, 2013). Security has been a serious challenge since the past and it still serves as the most vulnerable one. Burhan *et al.* (2018) presents main security issues commonly found in areas like ZigBee Technology, Bluetooth Technology, Radio Frequency Identification, Wireless Sensor Network, Wireless Fidelity and 5G Networks. In an ubiquitous computing environment, as sensitive information flows through such systems, the author believes that the need of a preventive mechanism to ensure the safety of information from the attackers is highly necessary during design process.

The main issue is that users are generally unaware when they come across many networks even if some harmful or insecure networks capture their personal or important information in the background. The widespread use of wireless devices have been the root cause of these challenges (Lyytinen *et al.*, 2004). Wireless infrastructure has some potential challenges, and these challenges could direct us to possible change or deletion, as well as denial of services. Wireless and mobile infrastructure security created from the use of various incompatible security schemes and inherent weakness in some wireless security algorithms (such as wireless LANs (Lyytinen *et al.*, 2004). Furthermore, poor execution, feature interactions, unplanned development, and new challenges that are created by prior attacks are also encountered in an ubiquitous environment. Furthermore, every ubiquitous computing device has an efficiency that is capable of saving power (i.e., sleeping mode), in this case attackers try to deal with this to shut down or reduce its efficiency. Even with the state-of-the-art technological advancement, the above issues persist and jeopardize the security in the ubiquitous computing environment. This is well defined and explained by Iwaya, Ahmad and Ali Babar (2020) who conducted a recent comprehensive study on ubiquitous health systems and its challenges. They pinpointed the security challenge to be a pressing need which needs a thorough comprehension during software development.

Since an infinite number of devices are connected in a ubiquitous computing environment, keeping track of them will also be harmful to the security of such systems. Many of the challenges relevant to the security concern have been identified in widespread literature and the key challenges can be consolidated as listed below;

- protection from unauthorized user (authorization),
- prevention of access by an attacker through unauthorized techniques (integrity),
- providing accessibility for user entirely (availability),
- avoiding an entity from refusing former actions (non-repudiation),
- confidentiality,
- authentication and
- accessibility.

Figure 02 further describes the security related issues as discussed by Shaheed *et al.*, 2015.

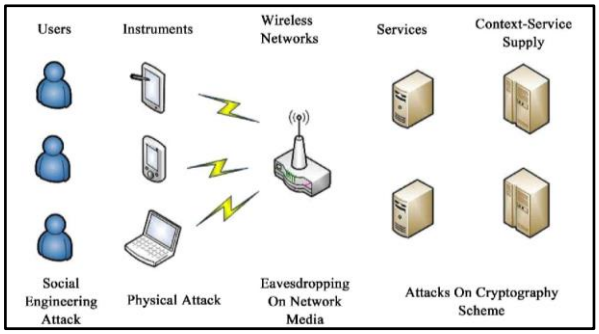

Figure 02: Ubiquitous environment and issues (Shaheed et al., 2015)

As security has been quoted as the most vulnerable issue, Malhotra *et al.* (2021) investigated the security perspectives in ubiquitous environments. The researchers forwarded a platform to deal with such issues through an understanding in proper detection and prevention of the attacks that are caused by the insecurity of the devices. The researcher gives a quick rundown of potential threats and anomalies at various levels and layers. Further research in this domain suggests a secondary line of defense in practical applications in addition to the cryptographic defense system that has a less addressing power on active attacks and exploitation of vulnerabilities. Based on this, Adat and Gupta (2018) proposed an Intrusion Detection System for an IoT scenario that can safeguard from security breaches if properly configured and built.

B. Social, Legal and Ethical Issues

Within a small period of time, Ubiquitous computing was able to adapt into human lifestyle easily in different forms. However, one of the grand challenges of ubiquitous computing is social, legal and ethical issues. Almost everyone carries a digital device with them at all times, whether it's a laptop, tablet, smartphone, or Etc. Data is available at all times and in almost any format the user wishes. Of course, this can be a benefit, but it might be difficult for someone seeking to safeguard customer privacy while providing uninterrupted service. As a result, businesses should think about it. Several authors have shown many issues in this category. Information privacy is frequently considered as an ethical issue in computing as being endangered by computing infrastructures that promote the transmission and use of personal data (Hilty, 2015). When more programs connect with the user, the user's privacy is jeopardized greatly (Shaheed *et al.*, 2015). The authors further mentioned that the main challenge is to provide a structure capable of changing daily living situations while also providing privacy to each individual user in an extremely dynamic pervasive environment. The study further stated that the trust is required for ubiquitous computing to demonstrate promising results. Based on the quote, “The substance that holds certainty and reliance on another's integrity and dependability is trust. In any interaction between nodes, trust is also a representation of dependability, security, and trustworthiness”. When it comes to privacy in ubiquitous computing, an interesting point that is worth mentioning is, users would be skeptical of such services if the ubiquitous devices upon which a flow is redirected kept track of flow details (Anjum, 2006). The author believes that providing such a guarantee might be a key challenge.

Another challenge those ubiquitous devices often face is legal issues as discussed by Chen and Tsai (2017). According to the researchers, trust concern is a key factor in ubiquitous manufacturing (UM) since UM generally involves multiple factories to manufacture a single product. In such contexts, there is a possibility of the leakage of technical secrets as a recipe is transferred from one factory to the other. This makes the legal issue a serious concern in Ubiquitous Computing as the stakeholders will not be willing to undertake ubiquitous manufacturing that causes legal concerns to the company. The interoperability based on mutual trust is an essential feature when

it comes to a manufacturing that is entirely ubiquitous. Thus, this makes the legal and ethical concern a grand challenge in Ubiquitous Computing.

An open debate exists on the use of location service in devices whether it is a violation of privacy or not. The usage of location to improve services can potentially be used to track users' whereabouts (Anjum, 2006). Location data is one of the most prevalent kinds of contextual data in the field of ubiquitous computing, and it is used to power a wide range of applications. The work of Jiang *et al.* (2021) is well-recognized in the field of location based services. They were able to identify practicality, quantification and personalization as the open issues that affect the performance when designing Location Privacy Preserving Mechanisms (LPPM). Furthermore, the authors believe that when it comes to Internet of Things (IoT) the existence of side channel data is the grandeur issue which developers should pay attention when designing such LPPMs. However, when location systems follow users automatically and in real time, a massive amount of potentially sensitive data is collected. Users might not necessarily want to turn off all access to their location data because some applications can benefit from it, but they do want to be in charge. So, when designing these ubiquitous devices, the developers should consider this challenge.

C. Technical Issues

Another grand challenge that ubiquitous computing has to overcome are technical issues. There are several technical challenges associated with ubiquitous computing such as performance, consistency, availability, designing, quality and testing (Anjum, 2006). Many researchers have addressed the technical issues encountered in a ubiquitous computing environment. The trade-off between consistency, availability, and resilience over a network split is one of the inherent challenges in making ubiquitous computing infrastructures expand to a huge number of people, devices, and sensors (Hong and Landay, 2002). Ubiquitous devices are capable of attracting many users simultaneously. The authors have proposed that the consistency, availability and partitioning should be taken into account as key challenges when designing ubiquitous devices. On the other hand, testing and evaluating such services will obviously present their own set of challenges. This is a difficult problem due to the intricacy of the services. As those services are expected to be used by a large number of people when they are deployed, investigating the influence of scalability on such services becomes an issue (Anjum, 2006).

The study has also discussed performance as one of the key challenges in the technical domain. According to the author, ubiquitous services must be delivered without compromising on the performance. The services, maybe in conjunction with the policies, will have to determine whether the available resources like bandwidth are adequate, and if not, then migrate to an interface with the necessary resources (Anjum, 2006). Davies and Gellersen (2002) focus their study solely on a branch of UM process which is deploying the systems. Authors have been able to explain the technical and sociological challenges of creating such systems that extend beyond just laboratory prototypes. The authors have provided an example and through that they make the point that even though the system can determine decisions there is a challenge to make the correct association between various components in providing this information. They further suggested, even though this process is easy for humans it is extremely difficult in software. Because there is lots of data that needs to be fed for the system in order to make a decision such as what criteria does the system use to decide and automate. Thus, a grasp of the delicate nature of the situation is essential. Before developing adequate defensive mechanisms, a system is absolutely necessary. As described by Malhotra *et al.* (2021) there are many ways to harm data integrity and confidentiality by hackers thus the need for a defensive mechanism of ubicomp development arises.

Chen and Tsai (2017) includes “quality” as a key challenge in ubiquitous computing. The authors explain the importance of quality and the problems and challenges faced by a factory when establishing a UM system. The author explains the composition of quality via an example which says that the parts of these ubiquitous computing equipment are made overseas. However, for the purpose of maintenance, a factory may be reluctant to wait for service from an overseas vendor. Instead, they would settle for a local business. This issue directly affects the quality of the UM. The authors mention that a remote diagnostic system can be used to overcome this challenge as it makes the vendor more prepared. One solution to overcome the above issue was forwarded by Hong and Landay (2002). A fact which is worth mentioning is, that just like a

recommender system does, end users must be able to easily review why a given action was made and adjust their preferred behavior for the system in a ubiquitous computing system because otherwise it would lead customers into confusion. According to them this is a key challenge when it comes to designing such systems. In a ubicomp setting, an end user may not notice an unwanted activity until much later after it has occurred. For these reasons, it will be beneficial to keep track of actions conducted on an individual's behalf, as well as a description of which device or services did the action, an explanation of why the action was taken, a method of quickly modifying the behavior, and tools for visualizing and interpreting the log.

D. Architectural Issues

The integration of a multitude of devices also challenges the architecture of ubicomp systems. Smart Homes are one such system designed to enhance people's lives by using ubiquitous computer technology that improves communication, awareness, and usefulness (Keith Edwards and Grinter, 2001). Hundreds of device manufacturers sell an extensive variety of products that are embedded in the home space, based on a multitude of technologies and specifications. This complexity has a strong impact on the rise in problems in Smart Homes. In the perspective of privacy in home automation systems, the usage of encryption keys in home automation deployments generates a slew of issues, including massive resource consumption and encryption key distribution efficiency (Batalla, Vasilakos and Gajewski, 2017). A cyber or physical assault by an enemy or even a malicious consumer might target various interactions among Smart Home entities (Komninos, Philippou and Pitsillides, 2014). As a result, the most prevalent challenges in ubiquitous computing are smart homes and associated potential risks and their probable implications. Adding more features to the protocol both raises the cost and decreases the protocol's simplicity of use (Risteska Stojkoska and Trivodaliev, 2017). Furthermore, ubicomp systems developers face an extreme issue when trying to fit their product to different kinds of environments. This situation is well described by Mirani *et al.* (2018). For an example, take an IOT home electronics manufacturing company. When designing their products, they simply cannot monitor each and every kind of home whether their environment suites the product or not. As stated in their paper this situation would create chaos and complexity for the ubicomp management. Furthermore, maintaining the systems would also be an issue. Still however, the most advanced glimpses of the potential future of domestic technologies can be found in home automation systems and challenges also increasing with it.

E. Challenges on human and environment

The challenge of Ubiquitous computing upon humans and the environment is unavoidable. As this technology has progressed, an unprecedented form of pollution in the form of electromagnetic radiation has been exposed to humans and has caused severe illnesses. Anyhow, human existence today would not be possible without electricity and telecommunication infrastructure (Lingvay *et al.*, 2018). We are enthralled by electromagnetic radiation because we use technology. This effect is extremely detrimental to everyone, regardless of age. According to Przystupa *et al.* (2020), the memory of infants suffers the greatest when they are exposed to low-intensity electromagnetic frequencies. The human immune system has a high level of sensitivity to electromagnetic frequency. However, the impacts of the built-up of the Ubiquitous computing idea on materials also present issues. Materials are concurrently subjected to many physical, chemical, and microbiological stress factors in built-up media, which operate synergistically with disruptive electromagnetic fields to promote material deterioration, with implications for building and installation durability and safety (Lingvay *et al.*, 2018). Thus, the impact of ubiquitous computing upon the environment is yet another challenge.

F. System Maintenance Challenges

As ubiquitous computers are becoming more and more into one system, the system maintenance employment problem have been emerging since the past. This forces the individuals to become an administrator for their own system. However, the individual does not possess potential capabilities to administer a system. At many instances, the users are not vigilant on security as well which may cause security threats & technical problems. Another challenge to consider is on the methodology to handle a large amount of data and how to allow users to search “effectively” for information in the ubiquitous environment (Lyytinen *et al.*, 2004). In these instances, there is a high possibility of information leakage even without the knowledge of users. Information

leakage by insiders is more problematic and crucial while the asset value of information is relatively higher. Therefore, it is most important to employ well trained administrators or an artificial intelligence bot to overcome this challenge which applies more strict control on internal information leakage whereas enabling staff inside the company to access internal information at any time in any place supporting high work efficiency. This issue is well described by Mirani *et al.* (2017) who makes a significant point by stating that the absence of system administrator is a pressing issue when it comes to ubicomp systems as when using such systems their users are lacking the knowledge on important concepts like the system's basic functionalities and performance. This necessitates the role of a system administrator to a ubicomp system.

V. DISCUSSION AND CONCLUSION

One way to define ubiquitous computing is "any-time" "any-where" access to computing resources. The nature of the ubiquitous environment allows communications and devices to traverse openly, anytime and anywhere, so modern computing networks have become increasingly ubiquitous. However, there are many challenges of ubiquitous computing to get its better performance. Therefore, this paper has summed up some grand challenges of ubiquitous computing with reference to extant literature available. The identified challenges can be listed as social, Legal and ethical issues, Technical issues, Application Issues, Challenges on human and environment, security challenges and System Maintenance challenges.

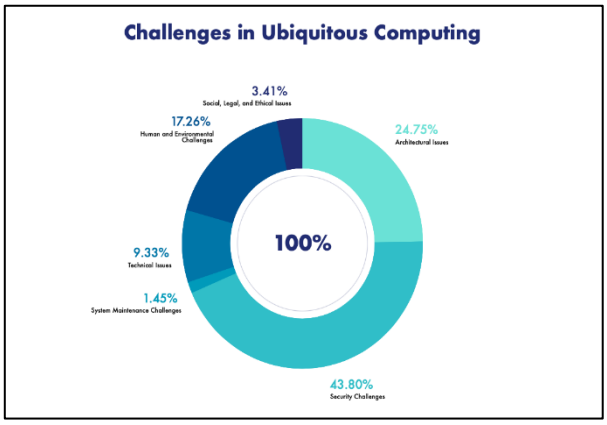

Figure 03: Challenges in ubicomp based on review

This study was able to identify major and trending challenges of ubiquitous computing. The critical analysis of the literature was able to categorize the challenges based on its impact and vulnerability. The challenges identified were ranked accordingly with the support of the scholarly articles. Social, legal and ethical issues were identified as the most challenging in ubiquitous computing whereas the impact on the human and environment was the least. The six challenges and their impact are illustrated in Figure 03.

Research interests of academics and industry are often quite different, however there are opportunities to produce good academic research that can assist industry (Prideaux, no date). Many ubiquitous applications these days are developed by the developers of the industry with the help from the research and development section, but academic researchers carry out exploratory studies in a systematic manner. If we could bridge the gap between the academic research and the relevant industry, we can build better applications. To develop errorless and robust ubicomp models we recommend to elegant designers by helping them see better work that goes into everyday security, trust and privacy. Hence, research in this field should build familiarity with the impacts of applying specific methods and should help selecting whatever design methodology is most appropriate for the configuration of current workload. To accomplish this objective, we propose to develop the security methodologies, debug the technological issues and make the model compatible with the environment. Many challenges we present here are sensible, applicable and within reach, making them prime challengers for rich future advancements. Our present study is limited with the Scopus database as Scopus is considered as the world's largest abstract and indexing database however, we plan to expand our research to undertake a systematic mapping study across various other databases in future.

REFERENCES

Adat, V. And Gupta, B. B. (2018) 'Security In Internet Of Things: Issues, Challenges, Taxonomy, And Architecture', *Telecommunication Systems*, 67(3), Pp. 423–441. Doi: 10.1007/S11235-017-0345-9.

Anjum, F. (2006) 'Challenges On Providing Services In A Ubiquitous, Mobile Environment', *2006 3rd Annual International Conference On Mobile And Ubiquitous Systems: Networking And Services, Mobiquitous*. Doi: 10.1109/MOBIQ.2006.340453.

Batalla, J. M., Vasilakos, A. And Gajewski, M. (2017) 'Secure Smart Homes: Opportunities And Challenges',

ACM Computing Surveys, 50(5). Doi: 10.1145/3122816.

Burhan, M., Rehman, R.A., Khan, B. and Kim, B.S., (2018) 'Iot Elements, Layered Architectures And Security Issues: A Comprehensive Survey', *Sensors (Switzerland)*, 18(9), Pp. 1–37. Doi: 10.3390/S18092796.

Chen, T. And Tsai, H. R. (2017) 'Ubiquitous Manufacturing: Current Practices, Challenges, And Opportunities', *Robotics And Computer-Integrated Manufacturing*, 45, Pp. 126–132. Doi: 10.1016/J.Rcim.2016.01.001.

Davies, N. And Gellersen, H. W. (2002) 'Beyond Prototypes: Challenges In Deploying Ubiquitous Systems', *IEEE Pervasive Computing*, 1(1), Pp. 26–35. Doi: 10.1109/MPRV.2002.993142.

Friedewald, M. And Raabe, O. (2011) 'Ubiquitous Computing: An Overview Of Technology Impacts', *Telematics And Informatics*, 28(2), Pp. 55–65. Doi: 10.1016/J.Tele.2010.09.001.

Hashemi, S. And Zarei, M. (2021) 'Internet Of Things Backdoors: Resource Management Issues, Security Challenges, And Detection Methods', *Transactions On Emerging Telecommunications Technologies*, 32(2), Pp. 1–25. Doi: 10.1002/Ett.4142.

Hilty, L. (2015) 'Ethical Issues In Ubiquitous Computing—Three Technology Assessment Studies Revisited', *Hilty, Lorenz (2015). Ethical Issues In Ubiquitous Computing—Three Technology Assessment Studies Revisited. In: Kinder-Kurlanda, Katharina; Ehrwein Nihan, Céline. Ubiquitous Computing In The Workplace. Cham: Springer, 45-60.*, (333), Pp. 45–60. Doi: 10.5167/Uzh-109998.

Hong, J. I. And Landay, J. A. (2002) 'Four Technological Challenges In Ubiquitous Computing And Their Influence On Interaction Design'.

Horváth, I. And Vroom, R. W. (2015) 'Ubiquitous Computer Aided Design: A Broken Promise Or A Sleeping Beauty?', *CAD Computer Aided Design*, 59, Pp. 161–175. Doi: 10.1016/J.Cad.2014.10.006.

Iwaya, L. H., Ahmad, A. And Ali Babar, M. (2020) 'Security And Privacy For Mhealth And Uhealth Systems: A Systematic Mapping Study', *IEEE Access*, 8, Pp. 150081–150112. Doi: 10.1109/ACCESS.2020.3015962.

Jiang, H., Li, J., Zhao, P., Zeng, F., Xiao, Z. and Iyengar, A.,. (2021) 'Location Privacy-Preserving Mechanisms In Location-Based Services: A Comprehensive Survey.', *ACM Computing Surveys*, 54(1), Pp. 1–36. Available At: Http://10.0.4.121/3423165%0Ahttp://Search.Ebscohost.Com/Login.Aspx?Direct=True&Db=Buh&AN=150035736&Site=Ehost-Live.

Keith Edwards, W. And Grinter, R. E. (2001) 'At Home With Ubiquitous Computing: Seven Challenges', *Lecture Notes In Computer Science (Including Subseries Lecture Notes In Artificial Intelligence And Lecture Notes In Bioinformatics)*, 2201, Pp. 256–272. Doi: 10.1007/3-540-45427-6_22.

Komninos, N., Philippou, E. And Pitsillides, A. (2014) 'Survey In Smart Grid And Smart Home Security: Issues, Challenges And Countermeasures', *IEEE Communications Surveys And Tutorials*, 16(4), Pp. 1933–1954. Doi: 10.1109/COMST.2014.2320093.

Lingvay, I., Bors, A.M., Lingvay, D., Radermacher, L. and Neagu, V. (2018) 'Electromagnetic Pollution Of The Environment And Its Effects On The Materials From The Built Up Media', *Revista De Chimie*, 69(12), Pp. 3593–3599. Doi: 10.37358/Rc.18.12.6800.

Lyytinen, K.J., Yoo, Y., Varshney, U., Ackerman, M., Davis, G., Avital, M., Robey, D., Sawyer, S. and

Sorensen, C. (2004) 'Surfing The Next Wave: Design And Implementation Challenges Of Ubiquitous Computing', *Communications Of The Association For Information Systems*, 13(July). Doi: 10.17705/1cais.01340.

Mahmoud, M. (2016) 'Ubiquitous Computing: Applications And Challenges', (April), Pp. 1–6. Available At: Https://Www.Researchgate.Net/Publication/311410466_Ubiquitous_Computing_Applications_And_Challenges.

Malhotra, P., Singh, Y., Anand, P., Bangotra, D.K., Singh, P.K. and Hong, W.C.. (2021) 'Internet Of Things: Evolution, Concerns And Security Challenges', *Sensors*, 21(5), Pp. 1–35. Doi: 10.3390/S21051809.

Mirani, A.A., Memon, M.S., Bhati, M.N., Soomro, M.A. and Rahu, M.A.,. (2017) 'Taxonomy Of Ubiquitous Computing', *2017 International Conference On Information And Communication Technologies (Icict)*, Pp. 202–208. Available At: Https://Ieeexplore.Ieee.Org/Stamp/Stamp.Jsp?Tp=&Arnumber=8320191.

Prideaux, B. and Campus, C. (2012) 'Bridging The Gap Between Academic Research And Industry Research Needs'.

Przystupa, K., Vasylkivskyi, I., Ishchenko, V., Pohrebennyk, V. and Kochan, O., (2020) 'Electromagnetic Pollution: Case Study Of Energy Transmission Lines And Radio Transmission Equipment', *Przeglad Elektrotechniczny*, 96(2), Pp. 52–55. Doi: 10.15199/48.2020.02.11.

Qiu, H., Kapusta, K., Lu, Z., Qiu, M. and Memmi, G.,. (2019) 'All-Or-Nothing Data Protection For Ubiquitous Communication: Challenges And Perspectives', *Information Sciences*, 502, Pp. 434–445. Doi: 10.1016/J.Ins.2019.06.031.

Risteska Stojkoska, B. L. And Trivodaliev, K. V. (2017) 'A Review Of Internet Of Things For Smart

Home: Challenges And Solutions', *Journal Of Cleaner Production*, 140, Pp. 1454–1464. Doi: 10.1016/J.Jclepro.2016.10.006.

Sen, J. (2010) 'Ubiquitous Computing: Potentials And Challenges', (February 2010). Doi: 10.13140/RG.2.1.3717.4005.

Shaheed, S. M. *Et Al.* (2015) 'Solving The Challenges Of Pervasive Computing', *Journal Of Computer And Communications*, 03(09), Pp. 41–50. Doi: 10.4236/Jcc.2015.39005.

Sharifi, A., Khosravi, M. And Shah, A. (2013) 'Security Attacks And Solutions On Ubiquitous Computing Networks', 3(4), Pp. 40–45.

Weiser, M. (1993) 'Ubiquitous Computing', *Computer*, 26(10), Pp. 71–72. Doi: 10.1109/2.237456.

Weiser, M., (1999) 'The Computer For The 21st Century'. ACM SIGMOBILE Mobile Computing and Communications Review, 3(3), Pp.3-11.