Literature Review on Current security Issues in Pervasive Computing

R.Jothi,M.Nikila,S.Gowri

*Department of computer Applications,Dhanalakshmi Srinivasan College of Arts and Science for Women,,Perambalur , 621 212, Tamilnadu, , India.

Email: jothi47859@gmail.com(R.Jothi*) Corresponding author:* R.Jothi

Abstract:

There has been a third wave of computing, and ubiquitous computing and communication has arisen from that wave. Pervasive computing and communication works with the environment to access services, information, or resources at any time and from any place. The user of this communication network is ignorant of the illicit usage of their sensitive data since the Pervasive objects are invisible to them. That data may be utilised or accessed by other devices connected to this network if the user is a smart one. As a result, the user now has greater room for security concerns. For the purpose of identifying unwanted access, this literature review examined and studied the most current privacy and security challenges. It examines the ubiquitous users' experiences with current security vulnerabilities and the potential dangers posed by the communication technology under consideration here. There are several issues that need to be addressed when it comes to preserving the privacy of our customers.

Keywords: Pervasive Computing, Smart device& networks, Security, privacy.

I.Introduction:

Our daily lives are now so intertwined with computers that they are able to think, detect, comprehend, and respond to our needs without our having to do anything. Smart gadgets in our everyday lives may create data in Pervasive Computing. In order to secure sensitive information, each device in the network must trust the user and offer the proper level of security.

In Pervasive Computing, the user may access the resources "anywhere and at any time" via a network of linked intelligent devices that automatically identify the external environment. [2] Because of their unique capabilities, these intelligent gadgets can take the role of desktop PCs. The special qualities of modern computing allow for simplified wiring, intelligent, invisible, and portable computing. Due of this environment's security concerns, the smart user is at risk. Smart devices and networks must be protected against significant security breaches.

The primary purpose of this literature review is to examine several studies in which probable security and privacy concerns of this environment may be studied and identified[3]. It may be used to evaluate the current security and privacy concerns by analysing current research publications.. It's laid out like this in the following way: provide an in-depth overview of this computing's fundamental and sub-properties in section1. Communication technologies have a significant impact on this ecosystem, thus discuss this topic in Section 2. Pervasive computing security topics are discussed in Section 3. Section 4: Examined the current privacy concerns. Detailed literature Review of Recent Papers to know the current security issues facing by the smart user of this environment for further research studies. At the end this paper may conclude the open security problem it may provide to help the further research directions.

II.Properties of PCE:

For Mark Weiser, this ubiquitous smart environment was all about the shared smart network, ambient awareness, intelligent iHCI and autonomously[4].[5] Mark Weiser Fig1 shows the sort of devices and systems that make up this PCE's core and sub-properties, which may be seen in this literature. Network distributed or shared Connected and clearly accessible gadgets allow users to engage with other connected devices as well as with people directly via a device's user interface. As long as users and other devices linked to the system are aware of the environmental context, devices may automatically obtain data from the physical environment. When it comes to artificial intelligence, devices may be able to handle a wide range of tasks and interactions without the need for human intervention. iHCI is implied in this case Implicit interactions between humans and computers are referred to as human-computer interaction (HCI). Intelligent gadgets are capable of operating on their own (ie devices have their own capable it will be work independently and make the decisions and actions by their own).

III.Communication Technologies:

Having a strong connection between a smart device and its user is crucial for the exchange of information between the user and other systems. The network might be wired or wireless. Wireless data exchange Figure 1 depicts the communication network’s basic characteristics.

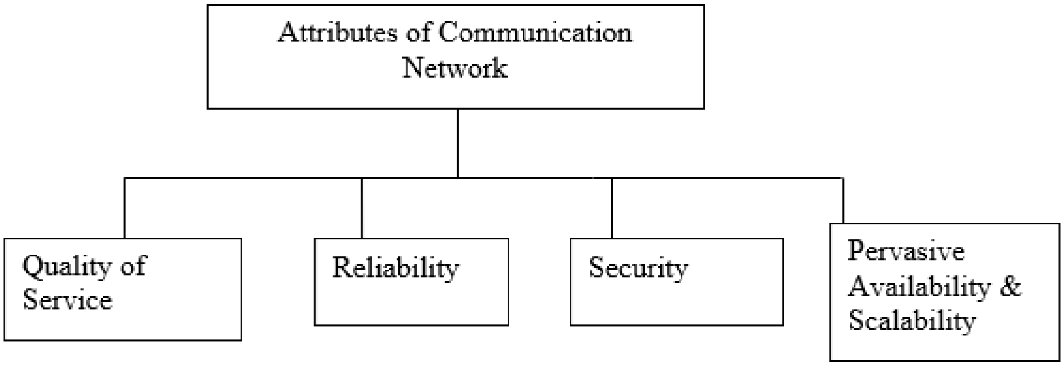
Attributes of Communication Network
Quality of Service
Reliability
Security
Pervasive Availability & Scalability

Figure.1. Communication Network

QoS (Quality of Service) is critical to data transit and exchange in a communication network. With the shared network's congestion in mind, it must assure the transmission of critical data. If the devices fail or the networks are congested, the communication network provides reliable and efficient data services. Ensure that the network is able to provide dependable service. Data security and privacy may be provided through communication networks. [6] It must be able to protect itself against assaults and illegal access, which is one of the most pressing issues on the network. So, in this report, we focus more on the network's most pressing refugee issues. The smart network's users may be found all over the world. All users of the network were connected at all times because of the network's efficiency in providing long-distance coverage. This smart network requires a certain number of sub- and distant devices to be linked. Because of this, the network's main strength is its potential to grow and be available to all users.

IV.Security

Smart technologies and communication systems are becoming more prevalent in our daily lives, and as a result, a corresponding rise in security concerns is inevitable. Security considerations such as Confidentiality, Integrity and Availability are critical when accessing smart ubiquitous devices, and the pervasive system will address these issues. Pervasive security phrases are demonstrated in the following figure 2.

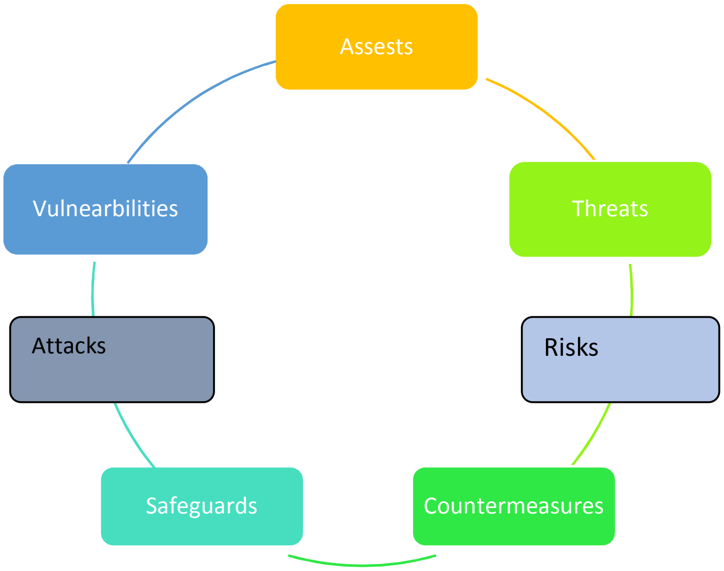

Figure.2. Pervasive Security

A risk evaluation of the ubiquitous environment against security threats can be addressed by all words in real life situations. When identifying an asset to safeguard, keep in mind that it might include anything from a smart gadget to a whole communication network or even the personally identifiable information (PII) of a smart user. Vulnerabilities: find out what makes a danger possible. Do you know the origins and routes of the problem? The threats may arise in a variety of ways.Risks: we can use risks to estimate the likelihood of an assault. The risk assessment has estimated the anticipated loss. As a result, all of the risk assessment terms play a significant part in the design of ubiquitous security systems.

V.Related works on Security Issues:

In order to identify the most pressing security concerns in ubiquitous computing, several publications were read and researched. In the next part, we'll explore a paper that deals with security concerns. Ameera Al-Karkhi and others[7] They explored privacy trust and identity as key issues on ubiquitous networks by analysing numerous publications to define the features of privacy and examining different techniques for protecting privacy. Traditional computing and widespread computing have been contrasted in terms of security concerns. Finally, new study avenues may be found in this smart environment's communication challenge. According to Lorenz M.Hilty et al ([8)], There are moral difficulties that must be addressed in this smart environment, and the ethics of modern computing have been recorded by decision making and self-evaluation, Control of authentication and sharing of the network infrastructure. Through the use of implanted devices, we were able to compare the results of our decision-making and self-evaluation to the current functioning conditions of this network. Smart devices and this platform are being used as a consequence of an authentication process.

Pervasive social networks were the subject of Takshi Gupta et al. [9]. On the topic of security difficulties and PON design issues, the author spoke. The study found a difficulty with security management via cryptographic mechanism-based security and security through access control-based mechanism-based management. In order to improve the security solutions, a detailed categorization has been offered.

Joseph Bugeja and others [10] The author addressed the privacy and security issues that arise in a smart home environment that is omnipresent. The difficulties are compared to issues with devices, communication, and service. The author discusses various solution approaches, including machine level, network level, and resource level approaches. In the words of Marco Conti and others[11], A number of Internet of People (IoP) research challenges are addressed in this paper, including node identification for communication, Multiple research questions are raised by the design of network architecture. IOP networking has a complicated algorithm and protocol framework. It's not an easy task to build a data management service from scratch.

Ema Kusen and colleagues Pervasive computing security issues were examined in detail by this author. In order to identify the dangers, vulnerabilities, and assaults they employed a methodical approach. Countermeasures to the user's issue, such as obtaining or erasing others' sensitive data, leaking others' resources, and using other device information, are described in this article. Several privacy-preserving strategies were discovered in this study, which may shield the smart user in this environment from being spied on and so saving the device resources. Numerous flaws in this ever-changing environment were identified by the author. Walaa elsayed et al. [13] cited in this article. Conventional access control methods have fundamental limitations, and this research reviewed how these approaches are not acceptable in a rapidly changing world. An access control model such as user/environment, user interaction, and service-based control models were all compared to see which was the most effective in the literature survey. In other words, Raja Naeem akramel al[14] There are many user-centered solutions presented in this article that synthesise the author's research on security, privacy, and trust. Security, privacy and trust in user-centric devices are among the unique challenges discussed in this study. The SPT literature survey for user privacy and malware detection reviews a large number of articles.

There are a number of security threats to the cyber-physical system, and these threats are analysed using three levels of architecture and comparing the problem faced on each layer. [15] Each layer's assessment and potential threats are examined.. An overview of CPS security threats, parameters, and countermeasures mechanisms was provided by the author. This article outlines various risk assessment options, including single- and multi-layer solutions.

Among them are Claudio Bettini and others

As a result of pervasive applications, privacy concerns have arisen. User movement-based services (e.g., smart advertisements), geographically connected network applications, sensing apps, pervasive healthcare, and smart home applications all have their own individual privacy threats and requirements. This paper discusses open research issues and challenges, including technical, user experience, and legal aspects and challenges.

Fisnik Dalipi [17] is a Serbian chess player. The author provides an overview of the challenges that smart environments face in terms of privacy and security. Stakeholder privacy and security, data and network security, and intelligent device privacy and security were all addressed in this article. The author tackled all three types of privacy and security issues. According to Qaisar Javid and his colleagues, The author examined a wide range of security and privacy concerns faced by today's ubiquitous users. Sifted through a number of papers and proposed existing security solutions, as well as addressing the various challenges of protecting sensitive information. A quality of service is achieved by summarising various existing solutions for widespread use. Syed miqsit and others[19] Unauthorized attacks on weak connections in an application's architecture, for example, were found in a prior investigation of ubiquitous computing interactions and problems. This article illustrates several solutions to the aforesaid difficulties, such as the role-based security solution and the trust-based security solution.

An in-depth analysis of security and privacy concerns on sensor networks was conducted by Alfredo J.Perez et al [20]. Data integrity and system availability are two of the categories in this article, as well as privacy challenges include reidentification context privacy and external data sharing. In this case, Muril Haque et al. [21] Confidentiality, availability and integrity of data in pervasive computing security policies are addressed in this paper by identifying various security issues, such as multiple interconnections between networks and the ability to identify the location of the smart user, providing authentication control for accessing the smart device; providing user privacy; the exchange of data between networks; and confidential feedback; The author found that the ubiquitous environment faced the following key difficulties.

Marconi Conti and others [22] Emerging technological and real-world problems were examined in this paper.. Because so much data is exchanged between environments, security must be implemented to protect both types of information. There are two security issues that the author addressed in this article, which include verifying the right user and modifying embedded devices and networks. Another consideration is the usability and security of pervasive device configurations. In order to protect the valuable data, privacy and confidentiality are essential. The authors have identified the above security issue in order to accomplish this goal.

At the end of the day, we're all in this together. Pervasive computing security and privacy challenges were examined in this research problem. Forensics and privacy proportions were among the topics covered in the various sections of this paper that focused on safeguarding the use of software in this environment. Some of these issues may increase security and privacy concerns in a pervasive environment.

Boshem et al[24] .'s Wi-Fi security in ubiquitous computing is addressed in this study. The IEEE 802.11 MAC Protocol is discussed in three ways. Such as CSMA/CA, VCS, and IEEE 802.11 state machines. The WiFi Security Timeline shows the year-by-year progression of wifi security protocols. Some of the most critical flaws have been uncovered, including ARP Spoofing, malicious code injection, and denial-of-service attacks. Using this easy method, the author claims that it is possible to diagnose any wireless issue related to WPA2 ARP Spoofing. ARP packets are safeguarded using the group terminal key mechanism. It is possible to detect all kinds of wireless ARP Spoofing using this steadfast approach.

a study by Priti Sharma and colleagues

Pervasive computing security was a key topic of discussion in the article. Users' privacy is one of the biggest concerns on this site because of the amount of context information that is given. Another concern is the node's ability to interact with dependable, secure, and trustworthy nodes on this autonomous network. Access network assaults, illegal connection attacks, data theft, and insider attacks are all examples of security breaches. In this study, Syed muqsit et al [25] deal with the most common ubiquitous computing security issues. Security, integrity, accessibility, and non-denial are some of the issues our present system must address. From trust and proficiency to social and user-based concerns are some of the biggest difficulties. As a result, this article provides a number of different security solutions for various types of users, such as access control that is dependent on the kind of user.

[26] Tarandeep and others

Complexity in the realm of ubiquitous computing arises in the design and development of high-performance pervasive systems. The author recognised the most important risk management in ubiquitous security as a result of this conversation. To improve security, it is necessary to eliminate threats and vulnerabilities. With an ubiquitous computing system, we can learn about the communication and security problems that may arise amongst tiny items and how they interact with one other. Possible dangers and flaws in the system It's important to think about potential risks and how to protect against them while creating a computer system.

It was Long Zhao Hua and others [27] who wrote this article In this paper, TePA (Tri element peer Authentication) was introduced as a mechanism to manage access control that can meet the specific needs of computing in order to overcome security issues. User satisfaction can be guaranteed by establishing a mutual trust. Proposals were made to use a WLAN network for the author's research. Make sure that all three parts of the network are connected to each other. Sensor networks are the primary use case for TePA. WVPHONE has implemented a TePA mechanism for IoT smart objects in this model TePA mechanism. Verifying users and services is possible. The security of modern computing is unquestionably enhanced by this method.

et al. [28]

Encryption algorithm using public key, Biometric data security (BS) and Cryptographic Algorithm by using visual scheme were proposed in this paper to provide high authentication of user of this environment (PKE) (VCS). The Zigbee IEEE 802.15.4 protocol-based sensor network used in this VCS Algorithm provides security against instructions. It is possible to utilise GSM and Wifi networks in a ubiquitous environment for a smart home monitoring system. The VCS Algorithm was used by the author to create a secure hash algorithm that is smart and efficient. Using this, it is possible to resolve many of the key concerns about the security of the modern house. The VCS algorithm serves as a bridge between different home appliances linked by a heterogeneous network and the smart home automation system.

Jiang and colleagues [29]

The notion of ubiquitous computer architecture was established by the author, who separated it into a series of layers. Some of the difficulties have been classified as important ones in this design. The gadgets in a ubiquitous computing environment are invisible to the smart user in the creation of this environment. Resource management and other service skills are the main concerns in this smart sector. One of the most pressing concerns in computing today is the transparency of connecting a device. An implanted version of the product may have an impact on the human body's biological environment. It is possible to recharge the battery using an integrated device [41-50]. The chemicals are released into the environment by the battery. As a result, it might pose a serious environmental threat.

VI. Summary of Security Issues and Challenges

S. No	Ref Papers	Major Security Issues and Challenges	Proposed Work
1.	Marianthi Theoharidou et al[31]	Loss of Confidentiality,Modification of Information,Loss of Availability, Repudiation ,Non-Auditability,Loss of Authenticity/Validity	Privacy protection framework regarding RFID services.
2.	Upkar Varshney et al[32]	Inability to authenticate and secure wireless channels, Difficulties of Access smart device(Device and network Attacks), possible loss, alteration of original data, and using others resources , modification of information, and denial of service.	Solution for secure wireless communication.
3.	Ivan Gudymenko et al[33]	Transparent Accessibility,Self-governess and Loss of Control problems.	Multilateral Security approaches**.**
4.	Tao Shu et al[34]	Privacy leakage in location based service.	Privacy-Preserving Location Calculation,Cryptographic Tool: Paillier Cryptosystem.
5.	Donia Bein et al[35]	Insertion Attacks, Interception sniffing attacks, Client – Client Intrusion Attacks.	Privacy Protection technique :Securing the data locally and securing communication
6.	Madhu Sharma Gaur et al[36]	Privacy issues,Trusted security,Social issues	Trust Computation Parameters: Trust

			Calculation and algorithm for trust evaluation.
7.	Stephen A[37]	Espionage, counterfeiting, sabotage, or privacy violations	Hopper-Blum Authentication protocol.
8.	Priti Sharma et al[38]	Third party attack, Accessing others Network , Usage of prohibited Connection , utilizing others Sensitive data, pinching Intermediary Device, Data Manipulation,DoS	Review on attacks.
9.	Pardeep Kumar et al[39]	Anonymity and unlinkability of Pervasive Device, Authentication and integrity,replay attack, impersonation attack.	Anonymou secure framework (ASF) for the smart devices /appliances.
10.	EmaKuˇsen et al[8]	DoS,Impersonation Attacks, Eavesdropping Attacks, Geo-Location Attacks, Cross Orgin Attacks, Malware.	Proposes a group of defense Mechanisms. Trust Computation and management, Encryption algorithm , Authentication and Access Control Mechanism.
11.	Yosef Ashibani et al[15]	Attacks on the sensor , GPS,RFID Attacks at the Wifi, Bluetooth, Inetrnet,LAN. Attacks at the smart device.	Single layer Solution, Multilayer Solution.
12.	Kahina et al	Goal Oriented Attacks, Performance Oriented Attacks, Layer Oriented Attacks.	Symmetric Cryptography Protocol, Asymmetric Cryptography Protocol.
13.	S. M. Shaheed et al.[25]	Privacy and Trust Issues, Social and User Interaction Issues	User Based Access Control, Trust Based Access Control.
14.	Bosheng Zhou et al[24]	ARP Poisoning, Injecting Malicious Code,DoS.	Group Terminal Key Encryption Technique.

15.	Priti Sharma et al[38]	Network Access Attack, Illegal Connection Attack, Device Stealing, Insider Attack.	Framework to Secure trustworthy environment.

VI. Conclusion

We can't imagine our lives without ubiquitous computing. The clever user of this environment has reaped the benefits of this technology to the fullest extent. Pervasive environment security and privacy are thus a must for safeguarding smart devices, smart networks, or sensitive data of any kind. Here, we discuss the smart environment's characteristics. Many studies examine and evaluate the risk assessment of this computing in order to identify the privacy and security issues. The review of current studies summarises and evaluates several existing systems. Finally, an overview of the security problems will bring an end to this document.

References:

[1]. Jason B. Forsyth, Thomas L. Martin,"Tools for interdisciplinary design of pervasive computing",International Journal of Pervasive Computing and Communications, Vol. 8, Issue 2, pp. 112-132,2012

[2]Hen-I Yang ,Chao Chen Bessam ,Abdulrazak Sumi Helal, "A framework for evaluating pervasive systems", International Journal of Pervasive Computing and Communications, Vol. 6, Issue. 4 pp. 432 – 481, 2010.

[3].Kayleen Manwaring et al,"Surfing the third wave of computing:A framework for research into eObjects ",Elsevier computer law & security review, Issue 3,pp: 586–603,2015.

[4] FahadKhan et al,"A Survey of Communication Technologies for Smart Grid Connectivity",**Proceedings of** International Conference on Computing, Electronic and Electrical Engineering (ICE Cube),2016.

[5] Vivian Genaro Motti," Users' Privacy Concerns About Wearables",Journal of International Financial Cryptography Association 2015, pp. 231–244.2015.

[6] Nigel Davies et al," Security and Privacy Implications of Pervasive Memory Augmentation" Journal of IEEE Pervasive Computing Volume: 14 , Issue: 1 , pp.44-53 2015.

[7]Ameera Al-Karkhi1, Adil Al-Yasiri2 and Nigel Linge3,"Privacy, Trust and Identity in Pervasive Computing: A Review of Technical Challenges and Future Research Directions",International Journal of Distributed and Parallel Systems , Vol.3,Issue.3,pp:197-218, 2012.

[8]Lorenz M. Hilty et al," Ethical Issues in Ubiquitous Computing – Three Technology Assessment Studies Revisited", Advances in Intelligent Systems and Computing. Springer,Vol.4,pp:206-218,2014.

[9]Takshi Gupta et al, "A Survey on the Security of Pervasive Online Social Networks",Journal of Internet Services and Information Security, volume: 8, Issue. 2 , pp. 48-86,2018.

[10]Joseph Bugeja, "On Privacy and Security Challenges in Smart Connected Homes",European Intelligence and Security Informatics Conference,Vol.4,pp.172-178,2016.

[11]MarcoConti et al," The Internet of People (IoP): A new wave in pervasive mobile Computing", Journal of Elsevier: Pervasive and Mobile Computing ,Volume 41, pp. 1-27,2017.

[12]EmaKuˇsen et al, "Security-related Research in Ubiquitous Computing – Results of a Systematic Literature Review", Journal of cryptography and security, Vol.8,pp.1-18,2016.

[13]T. Gaber et al.," Access Control Models for PervasiveEnvironments: A Survey" ,The Journal of 1st International Conference on Advanced Intelligent System and Informatics ,pp.511-522,2015.

[14]Raja Naeem Akram et al,"Security, privacy and trust of user-centric solutions", Journal of Future Generation Computer Systems, Vol.80,pp.417-420,2018.

[15]Yosef Ashibani *, Qusay H. Mahmoud,"Cyber physical systems security: Analysis, challenges and solutions", Journal of computers & security , Vol.68 ,pp.81–97,2017.

[16]Claudio Bettini,"Privacy protection in pervasive systems: State of the art and technical challenges", Journal of Elsevier: Pervasive and mobile computing, Vol 65,pp.1-16,2015.

[17]Fisnik Dalipi,"Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges", Proceedings of 4th International Conference on Future Internet of Things and Cloud Workshops, 2016.

[18]QAISAR JAVAID* et al,"Dissecting the Security and Protection Issues in Pervasive Computing",Mehran University Research Journal of Engineering & Technology
Vol. 37, No. 2, pp.241-256, April 2018.

[19]Shaheed, S.M., Abbas, J., Shabbir, A. and Khalid, F.," Solving the Challenges of Pervasive Computing", Journal of Computer and Communications, vol.3, pp.41-50,2015.

[20]Alfredo J. Perez et al,"Security and Privacy in Ubiquitous Sensor Networks",Journal of Information Processing System, Vol.14, Issue.2, pp.286-308, April 2018 .

[21]Munirul Haque et al,"Security in Pervasive Computing: Current Status and Open Issues",International Journal of Network Security, Vol.3, No.3, PP.203–214, 2006.

[22]Marco Conti et al,"Looking ahead in pervasive computing: Challenges and opportunities inthe era of cyber–physical convergence",Journal of Elsevier:Pervasive and Mobile Computing ,vol.8,pp. 2–21,2012.

[23]Apostolos Malatras et al,"State-of-the-art survey on P2P overlay networks in pervasive computing environments",Journal of Network and Computer Applications ,vol.55,pp.1–23,2015.

[24]Bosheng Zhou et al,"Wireless Security Issues in pervasive computing", proceedings of Fourth International Conference on Genetic and Evolutionary Computing, 2010.

[25] Syed Muqsit Shaheed et al,"Solving the Challenges of Pervasive Computing",Journal of Computer and Communications, vol. 3,pp. 41-50,2015.

[26]Tarandeep Kaur et al,"Security Issues In Design And Development of High Performance Ubiquitous Computing", Sixth International Conference on Computational Intelligence and Communication Networks,2014.

[27]Long Zhao hua et al,"Research on Pervasive Computing Security",Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing,2010.

[28]M Varaprasad Rao,"Secured Smart System Desing In Pervasive Computing Environment Using Vcs",International Journal of UbiComp (IJU), Vol.6, Issue .2, pp.13-19, 2015.

[29]Jiang Dai et al,"Pervasive computing architecture, key technologies and issues facing", Journal of Applied Mechanics and Materials, Vol.3,pp 684-687 ,2012.

[30]Leonardo B. Oliveira et al"The computer for the 21st century:present security & privacy challenges"Journal of Internet Services and Applications, pp.9:24,2018.

[31] , Marianthi Theoharidou et al ,"Privacy in Ubiquitous Computing Infrastructures", Journal of Information Security and Critical Infrastructure Protection,2016,

[32]Upkar Varshney et al,"Network Access and Security Issues in Ubiquitous Computing", Journal of IEEE Pervasive Computing, vol.4,issue.5,pp.26-32,2015.

[33]Ivan Gudymenko et al," Privacy in ubiquitous Computing", Proceedings of International conference on smart device security,2014.

[34]Tao Shu et al,"Protecting Multi-Lateral Localization Privacy in Pervasive Environments" ,IEEE/ACM Transactions On Networking, Vol. 23, No. 5, pp.1688-1699, 2015.

[35]Donia Bein et al," Wireless communication in Ubiquitous Computing an Easy Target to attack", Journal of Scientific Research, Vol. 4 ,Issue 3,pp153-160,2011.

[36]Madhu Sharma Gaur," Trusted and secure clustering in mobile Pervasive environment",

A Springer Journal :Human Centric Computing and information Scienece",vol.5 ,Issue.3,pp.1-17,2015.

[37]Stephen A. Weis,"Security Parallels Between People and Pervasive Devices", Journal of Computer Science and Artificial Intelligence, Vol.5,Issue.2,pp.1-15,2014.

[38]Priti Sharma et al,"Security Issues in Ubiquitous Computing: A Literature Review",International Journals of Advanced Research in Computer Science and Software Engineering,Volume-7, Issue-8,pp.17-20,2017.

[39]Pardeep Kumar et al,"Anonymous Secure Framework in Connected Smart Home Environments"IEEE Journal of Transactions on Information Forensics and Security,VOL. 13,Issue. 9, 2014,pp.1-12.

[40]Bodei, C., Degano, P., Ferrari, G-L., Galletta, L., & Mezzetti, G., "Security in Pervasive Applications: A Survey", European Journal of Law and Technology, Vol. 4, No. 2, pp.1-11,2013.

[41] Rangaraj, R., Sathish, S., Mansadevi, T. L. D., Supriya, R., Surakasi, R., Aravindh, M., ... & Osman, S. M. (2022). Investigation of weight fraction and alkaline treatment on catechu linnaeus/Hibiscus cannabinus/sansevieria ehrenbergii plant fibers-reinforced epoxy hybrid composites. Advances in Materials Science and Engineering, 2022.

[42] Ganesh, S. S., Kannayeram, G., Karthick, A., & Muhibbullah, M. (2021). A novel context aware joint segmentation and classification framework for glaucoma detection. Computational and Mathematical Methods in Medicine, 2021.

[43] Munimathan, A., Sathish, T., Mohanavel, V., Karthick, A., Madavan, R., Subbiah, R., ... & Rajkumar, S. (2021). Investigation on heat transfer enhancement in microchannel using Al2O3/water nanofluids. International Journal of Photoenergy, 2021.

[44] Aravindh, M., Sathish, S., Ranga Raj, R., Karthick, A., Mohanavel, V., Patil, P. P., ... & Osman, S. M. (2022). A Review on the Effect of Various Chemical Treatments on the Mechanical Properties of Renewable Fiber-Reinforced Composites. Advances in Materials Science and Engineering, 2022.

[45] Hmidet, A., Subramaniam, U., Elavarasan, R. M., Raju, K., Diaz, M., Das, N., ... & Boubaker, O. (2021). Design of efficient off-grid solar photovoltaic water pumping system based on improved fractional open circuit voltage MPPT technique. International Journal of Photoenergy, 2021.

[46] Rajendran, V., Ramasubbu, H., Alagar, K., & Ramalingam, V. K. (2021). Performance analysis of domestic solar air heating system using V-shaped baffles–an

experimental study. Proceedings of the institution of mechanical engineers, part E: journal of process mechanical engineering, 235(5), 1705-1717.

[47] Sathish, T., Mohanavel, V., Karthick, A., Arunkumar, M., Ravichandran, M., & Rajkumar, S. (2021). Study on Compaction and machinability of silicon nitride (Si3N4) reinforced copper alloy composite through P/M route. International Journal of Polymer Science, 2021.

[48] Kumar, R. R., Thanigaivel, S., Dey, N., Priya, A. K., Karthick, A., Mohanavel, V., ... & Osman, S. M. (2022). Performance Evaluation of Cyclic Stability and Capacitance of Manganese Oxide Modified Graphene Oxide Nanocomposite for Potential Supercapacitor Applications. Journal of Nanomaterials, 2022.

[49] Sujith, A. V. L. N., Swathi, R., Venkatasubramanian, R., Venu, N., Hemalatha, S., George, T., ... & Osman, S. M. (2022). Integrating nanomaterial and high-performance fuzzy-based machine learning approach for green energy conversion. Journal of Nanomaterials, 2022.

[50] Pazhanimuthu, C., Baranilingesan, I., & Karthick, A. (2021). An improved control algorithm for series hybrid active power filter based on SOGI-PLL under dynamic load conditions. Solid State Communications, 333, 114357.