Research Issues And Challenges Of Pervasive Computing

M.Kamarunisha,R.Jothi,P.Anitha

**Department of computer Applications,Dhanalakshmi Srinivasan College of Arts and Science for Women,,Perambalur , 621 212, Tamilnadu, , India.*
Email: kamarunisha8891@gmail.com *(***M.Kamarunisha***) Corresponding author:* **M.Kamarunisha**

ABSTRACT

Computer applications that are omnipresent or "pervasive" are examined in this research for their security concerns. At any moment, any small or wearable gadget may receive service. New opportunities and challenges for Information Technology companies arise when high-performance computers and sensors are incorporated into practically every piece of equipment in buildings, home care, Intelligent transportation system workplaces and industries as well as in clothing. Conventional networked applications have many of the same security issues as PCEs. There are also security measures in place to secure data or information such as passwords, usernames and passwords and other forms of authentication.. Finally, real-time applications are used to debate the future of ubiquitous computing.

Keywords: Pervasive computing, intelligent transportation;trojan horses.

1 INTRODUCTION

All three domains of pervasive computing are covered by pervasive computing: It's about how people see and utilise mobile computing devices in their everyday lives. It has to do with the creation and deployment of programmes that make it possible to carry out such operations. As new knowledge and capabilities become widely available, they enrich the environment in which we live. Pervasive computing environments make life easier by allowing devices to move about and offering a digital infrastructure that can give beneficial services to individuals in the environment, whenever and wherever they need them [6-10]. There are several hazards and security concerns that have not before been experienced in more conventional computer settings while using ubiquitous computing. Designers of these ecosystems face new challenges, including those related to privacy, trust, and identification. The system must be able to consistently and confidently identify the user who wants to use the environment's resources in order to design secure ubiquitous environments. Establishing and validating the identification of users in such situations entails significant dangers, which must be taken into consideration. Additionally, users need to feel secure in the knowledge that their personal information will not be abused in any manner they do not consent to. Such settings need a high level of privacy since the system must be regarded by the user as being protective of their data.

2. Characteristics and Architecture of Pervasive Computing

There are a number of characteristics and capabilities that may be used to categorise pervasive computing. It is envisaged that mobility and ad-hoc networking capabilities will be available within the next year or two. Characteristics like as autonomy, context awareness, and energy autarky are estimated to take anywhere from five to 10 years to develop. [1]. Pervasive computing's ultimate and deciding properties are considered as context awareness and embedding in everyday things. All man-made and some natural objects will eventually have hardware and software as a consequence of computer technology progressing at an exponential rate. [2] From clothes and tools to automobiles, houses, and even your coffee cup, chips may be embedded in practically any

object to link it with an unlimited network of other devices. Pervasive computing is a notion that extends beyond personal computers. For ubiquitous computing to be successful, it has to be integrated into the environment in a manner that the connection of devices is inconspicuous and constantly accessible. This may be achieved by using wireless computing, speech recognition, Internet capabilities, and artificial intelligence is shown in figure 1.

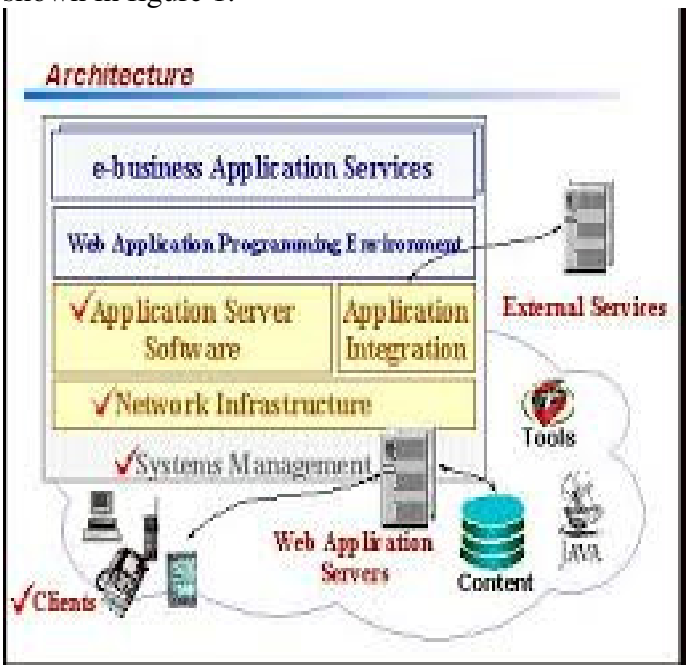

Figure.1. Architecture

3.Pervasive Computing Applications

Pervasive computing has the potential to have a profound impact on society, businesses, and individuals. [3] Quality of Life, Quality of Experience, Convenience, Return on Investment, and Assistance are among the most common high-level objectives of such apps.. Aging, Disabilities, and Independence (ADI), a Quality of Life (QoL) issue for the elderly and others with special needs, is one of the world's major research institutes in ubiquitous computing. ADI research needs a wide range of expertise that cannot be obtained without collaborating with other researchers (including international). Proactive health applications of ubiquitous computing with an emphasis on persuasive tele-health systems is another multidisciplinary research topic that the lab investigates in depth is shown in figure 2.

Using plants that naturally filter the air in a little greenhouse in the house, it delivers fresh air and a pleasant natural aroma to the home.

Figure.2. Pervasive Computing

The greenhouse automatically regulates the temperature and humidity in order to alter the plants' purifying powers to meet the needs of the house's pollution level [3]-[5].

The Smart Floor, a residential-grade, raised tile system, is the principal location tracking technology in the home. One square foot of each tile has a pressure sensor installed underneath it. The Smart Floor, unlike other monitoring technologies, does not need the occupants' attention, any wearable devices, or cameras that violate their privacy. The Smart Floor is highly handy for the user since it is unencumbered and does not need any human attention. Because it silently and discreetly gives rich awareness of location and activity for the Smart House, the Smart Floor is quite useful.

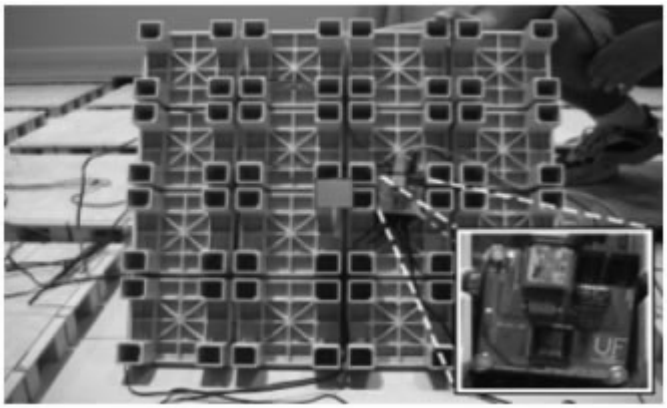

Figure.3. Smart Floor

Using the Smart Floor API, other smart home apps may access location and activity services. The location service is used by applications when they require location contexts. Others, such as daily activity counters that count and report the total number of steps taken by a person, are totally location-based (e.g. care giver, or a relative). Also offered is an implementation of the location service in a phenomenon cloud that improves the service's overall dependability even when sensors malfunction or produce a considerable amount of noise is shown in figure 3.

In the event that someone is unable to determine the meaning of an unfamiliar word, they may use a smart pen to look it up reading books .

Figure.4. Foreign Language

For papers written in a foreign language, this is very handy. Simply highlight or write down the unfamiliar word, hit the translation key, and then the pen will automatically project the translation onto a paper in your hand. For papers written in a foreign language, this is very handy. Simply highlight or write down the unfamiliar word, hit the translation key, and then the pen will automatically project the translation onto a paper in your hand is shown in figure 4.

The SmartWave comprises of a microwave oven, as well as various gadgets and services that help with meal planning. The SmartWave is able to identify properly labelled frozen meals thanks to an RFID reader installed beneath the counter top below the microwave. A monitor above the microwave displays the essential instructions for the homeowner to prepare the food (remove film, stir ingredients, etc.). Multi-cycle cooking (e.g. thawing, low-power followed by high-power) is no problem with the SmartWave. Cooking times and power le-

vels are set automatically. A notice is delivered to the resident once the meal is ready, no matter where they are in the home. People with vision problems who are unable to read the small type on the frozen food labels would benefit greatly from this technology. Those who have manual dexterity issues or mild dementia benefit from it as well.

The fundamental purpose of the Cognitive Assistant (CA) project is to help older persons with mild dementia overcome challenges in carrying out basic daily tasks by means of reminders, direction, and context-sensitive triggering.. Attention Capture and multimedia cueing are provided by the cognitive assistant inside. Detachment from particular material and events makes the assistant a broad service. In the Smart House, this may be used for any application that needs reminders, training, or cueing. In the past, the CA has been utilisedas a proactive reminder for chores that are important (to take medications, to eat at meal times, to go see the doctor, to call son on his birthday, or to feed the pet). It's also been used to teach people how to do things step by step (specifically in re-training on hygiene tasks). The SmartWave was used to prepare a meal and ensure proper hydration as an example of behaviour modification. CA has also been used as a means of keeping tabs on the elder's activities [11]-[17].

This kind of environment can detect and identify the devices and services it has access to, evaluate their condition, and then engage with them to change them if necessary. Self-sensing, for example, is a service that gives a real-time model of the state of all the appliances in the Gator Tech Smart House, for example. Prerequisite service for self-sensing is the SmartPlug. A low-cost RFID reader is hidden behind the plug hardware in the wall of the Smart Plug, which is a regular power outlet. Devices, such as a light or a fan, are given RFID tags that hold information about them. Pass-through plugs now have RFID tags (the white cubical below). After plugging an appliance into the pass through cube, the equipment's RFID tag is read and its location identifier is determined. This dynamic information is immediately available to the home. The plug may be activated by adding a sensor node to it. Switching the appliance on and off is the only action permitted.

Getting out of bed in the morning may be a stressful experience in today's fast-paced world, but with the help of a smart bed, you can make a stressful experience more pleasant.

A pillow that could meet all of your bedtime requirements would be perfect.
A smart pillow may read to you at night and play your favourite music to help you fall asleep when you're feeling drowsy.
Researchers in the social and life sciences, including doctors and other health care professionals, have long wanted the capacity to monitor study subjects or patients for a range of illnesses or disorders on a continuous basis. Behavioural modification practises for both psychological and medical therapy employ monitoring data to change treatment dose or regimens in real time. Mobile and Pervasive Computing has organised a multidisciplinary team to investigate tele-health solutions for obesity and diabetes. Traditional tele-health delivery models have been examined by us and we feel we've made significant advancements to the concept that we believe will reinvigorate it. Our research so far has focused on the need to add two strong capabilities to telehealth systems: (1) behaviour recognition, which is powerful sentience above and beyond vital signs and activity sensing, and (2) persuasion and adaptive persuasion loops, which is powerful (human) actuation. As a result, we anticipate that tele-health systems will become more effective and efficient with the integration of both sentience and actuation. Currently, we're focusing on persuasion and tele-health participatory behaviour recognition. As part of our research, we propose to conduct a large-scale validation of our hypothesis.
It happens to the best of us: forgetting a key item at home that you need for the day.
As a result, you'll never again have to worry about forgetting something because of this smart Gate reminder.

The sleek dressing table is a must-have item for ladies who are fed up with putting their makeup on in a dark and dingy setting in the morning. Using this dressing table, the user is able to swiftly and easily apply their makeup in the most efficient manner possible [18-27].

Whether or whether a member of the family is approaching the house is indicated through a cordless communication system.

Additionally, it offers convenience and may serve as a safety net for members of the family by helping them communicate and bond better. It consists of a transmitter and a receiver that may be taken anywhere. When a member of the family approaches the home, this gadget bursts into blossom. People inside and outside of the home may benefit from this innovative technology is shown in figure 5.

Figure.5. Technology Applications

According to some businesses, "epaper" will replace paper books and newspapers in the future. Because it's so tiny, you could carry it in your pocket like a normal computer display. Changing a display's size might be a challenge. Displays are continuously becoming larger, so how can we use them more effectively?

At the entryway of a home, a mat serves as a critical link between the interior and the exterior of the house.

The smart mat is able to identify the person who is treading on it based on their body weight and footprint.

It's fairly uncommon to hear the term "pervasive computing" used in reference to healthcare.

Consumer monitoring equipment such as blood pressure cuffs and glucose metres, which may be connected to a personal computer, are often used in these scenarios.

In order for healthcare providers to learn more about their patients' everyday lives, they must gather patient data in a variety of contexts outside the doctor's office.

A third significant scenario is in emergency treatment, when medical information may be accessed quickly or specialists can be sent to the spot remotely. We believe that by providing medical professionals with accurate and thorough information, we can help them provide better treatment that is tailored to the patient's specific needs and history. Much attention has been paid to the surgical profession due to the high stress levels that

surgeons and nurses are under. Systems for collecting and analysing telemetry from operating room devices are being developed by technologists in order to enhance human abilities to notice patterns of concern that may need rapid intervention.

Many of these applications have been well publicised and are already being implemented. Home PCs and consumer products may readily connect to one other, allowing consumers to collect data from sensors in their homes that can be accessed online by their doctors from anywhere. Remote doctors are now able to advise on a patient's health and participate in a surgical operation through telesurgery. These "anticipated" uses are not the focus of this special issue, which aims to show readers how ubiquitous computing technology may be used in a broad variety of healthcare settings. There are at least three benefits to ubiquitous computing that proponents claim:
Aiming to reduce healthcare costs by delivering appropriate treatment to those in need more quickly; 2. Expanding access to high-quality healthcare to more people; and 3. Making healthcare more individualised, encouraging individuals to take more responsibility for their own well-being.

4. SECURITY CHALLENGES

Traditional networked applications have many of the same security concerns as PCEs. In addition, they include device and user authentications, data or information privacy, protection against dangerous code such as viruses, worms and Trojan horses, and access control techniques.. Pervasive computing does bring some new challenges to an already complicated security area, though. Physical security is critical since the gadgets might be easily lost or stolen. It's possible that data that was formerly kept inside a corporate firewall is now circling the internet, stopping at hosted servers or wireless gateways along the route is shown in figure 6. .

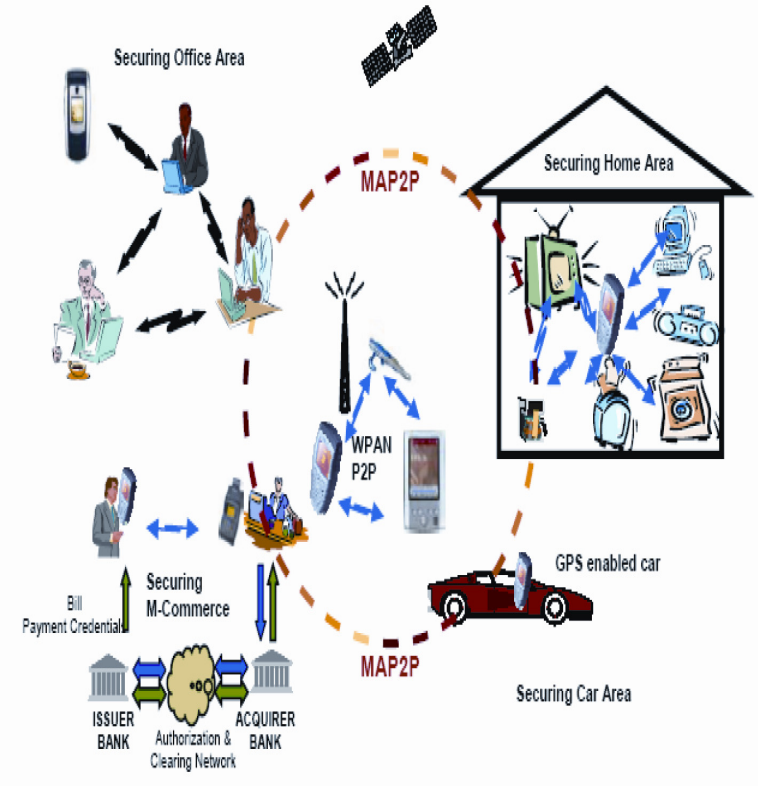

Figure.6. Security Challenges

Traditional security principles and solutions have been applied to a wide range of ubiquitous platforms. As a result of this, the security architecture has to be reworked a great deal in order to fit in with the ubiquitous framework, which increases the danger of new breaches. The necessity for a general security framework cannot be overstated. When developing ubiquitous computing frameworks, it is important to detect potential security risks early in the process. To name a few, there are:

There are more sites of failure in pervasive systems than in typical computer settings [2]. Pervasive systems will swiftly become mission important if people rely on them to mediate their day-to-day activities. They must be sturdy, reliable, and constantly accessible to ensure their success. A widespread computing framework will have a tough time dealing with this issue. Risks to service dependability will rise because of the large range of computer technologies that will be used by organisations.

New security issues arise when a ubiquitous computing system is supported by a new infrastructure, such as in the area of trust management [6, 7]. When an unknown entity, such as a PDA, mobile phone, or laptop computer, provides services, the question of trust will come to the surface. A company that provides services may have a long-standing relationship and be trusted. Because it is the first time connecting to a ubiquitous environment, an entity does not have any prior history to rely on when trying to gauge its trustworthiness. For example, a person or organisation might be evil and disrupt services, or they could be seeking to use a certain service. This raises the issue of whether or not current members of the ecosystem are confident in this new entity's intentions. New entities (A and B) linked to the ubiquitous environment may, for example, want to share data. Do they have faith in each other? Traditional computer environments [2] are not supported. Mission-critical systems will emerge if individuals rely on ubiquitous systems to moderate their daily activities. They must be sturdy, reliable, and constantly accessible to ensure their success. A widespread computing framework will have a tough time dealing with this issue. Risks to service dependability will rise because of the large range of computer technologies that will be used by organisations.

A Denial of Service (DoS) attack is a typical kind of malicious assault. To put it another way, a Denial-of-Service (DoS) assault is an attack on a network resource that prevents legitimate users from using it [9]. DDoS attacks are coordinated attacks on the availability of services of one target system or network that are launched across several infected computers [10]. An assault by an entity linked to the ubiquitous computing framework will be possible. Intentionally trying to access a service that isn't intended for them is a common kind of harmful behaviour, and it may happen to anybody. In addition to causing the innocent entity to malfunction, a DoS attack may also create additional issues, such as excessive network latency, scalability issues when new entities attempt connecting to the framework, and service unavailability.

It is possible for data to be damaged or tampered with when it is communicated between entities. The integrity of data in a ubiquitous environment must be maintained at all times. Data that has been tampered with may go undetected by the entities involved.

Because ubiquitous systems will mediate ordinary physical action, technological procedures to allow recourse must be built-in from the beginning[2], says Ranganathan. There's an issue when one of the parties to a service agreement backs out before it's completed. Mechanisms to cope with this should be included into a ubiquitous computing architecture. Toward the end of this part, we'll present a ubiquitous computing framework called ConStruct. When discussing security problems in an ubiquitous setting, we utilise this to get people talking.

Two dimensions of data privacy are involved. Firstly, it has to make sure that any active or passive attackers aren't able to access the data that is being shared or exchanged in any way[18-27]. There are a variety of encryption and decryption methods to consider from the start. But at the same time, we need to keep in mind the constraints of memory, battery life, and other aspects of the device. Users in a ubiquitous computing environment, on the other hand, have a considerably greater degree of flexibility and control over their movement. From well-protected to completely open and unprotected settings, this encompasses a wide range of conditions that make the problem of protecting data even more difficult. Secondly, how can it be certain that the user data that is being gathered nearly certainly will not be utilised maliciously? How can we be confident that the complex data is not being handled by any unauthorised person?

The evident peculiarity of the ubiquitous computing ecosystem is its mutual collaboration, interconnection, and interdependability. In addition, there is the question of trust. By sharing data with an unauthorised device, the likelihood of a data breach increases. [8].

6.CONCLUSIONS

Pervasive/ubiquitous computing is a fruitful source of hard problems in computer systems today, and the material provided in this Paper is a good starting point for further research. Research in the future will concentrate on developing applications such as smart homes or offices or universities employing improved embedded systems or efficient soft computing approaches without any technological difficulties. Instead of serving as a repository for proprietary code, devices should be seen as gateways to the application and data space enabled by the environment. Apps should not be seen as programmes developed just to take use of a computer's resources, but rather as activities that a user may benefit from. There are many different types of services that may be supported by a ubiquitous computing architecture. It is quite likely that most organisations have little or no understanding about the services provided by other organisations. When a new company launches a new service for the first time, this raises significant security concerns. There is a significant expectation that a ubiquitous computing framework will be able to offer acceptable security for all entities in this environment because of the 'unknown' aspect. These entities can interact with one other without needing to know anything about the framework. It's possible that entities will be reluctant to connect to and use services in the framework if they don't know how to protect themselves.

7. REFERENCES

1.http://en.wikipedia.org/wiki/Pervasive_Computing

2.Lathies Bhasker T “Pervasive Computing Issues, Challenges andApplications”International Journal Of Engineering And Computer Science ISSN: 2319-7242Volume 2 Issue 12, Dec.2013.

3.**“Security Issues with Pervasive Computing Frameworks”**Michael CollinsSystems Research Group, School of Computer Science and Informatics,UCD Dublin, Ireand.

4.”Issues and challenges in ubiqutious computing”
Protocol Engineering & Technology (PET) Lab.
Indian Institute of Science,Bangalore.

5.https://www.google.co.in/search?q=pervasive+compuing+characteristics&biw.

6.A Survey on Pervasive Computing Er. ManitaGorai, Er. KamnaAgarwal,International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012

7.M. Satyanarayanan: Pervasive Computing: Vision and Challenges. IEEE Personel Communications, 2001

8. Bakre, A., Badrinath, B.R. Handoff and System Support for Indirect TCP/IP. In Proceedings of the Second Usenix Symposium on Mobile & Location-Independent Computing. Ann Arbor, MI, April, 1995.

9. Bhagwat, P., Perkins, C., Tripathi, S. Network Layer Mobility: An Architecture and Survey. IEEE Personal Communications 3(3), June, 1996. 10. Birrell, A.D., Nelson, B.J. Implementing Remote Procedure Calls. ACM Transactions on Computer Systems 2(1), February, 1984.

11. Borg, A., Blau, W., Graetsch, W. Fault Tolerance Under Unix. ACM Transactions on Computer Systems 7(1), February, 1989.
12. Brewer, E.A., Katz, R.H., Chawathe, Y., Gribble, S.D., Hodes, T., Nguyen, G., Stemm, M., Henderson, T., Amir, E., Balakrishnan, H., Fox, A., Padmanabhan, V.N., Seshan, S. A Network Architecture for Heterogeneous Mobile Computing. IEEE Personal Communications 5(5), October, 1998.
13. Brodersen, R.W. InfoPad — past, present and future. Mobile Computing and Communications Review 3(1), January, 1999.
14. Case, J., Fedor, M., Schoffstall, M., Davin, J. A Simple Network Management Protocol. Internet Engineering Task Force (RFC 1157), 1990.
15. Couloris, G., Dollimore, J., Kindberg, T. Distributed Systems Concepts and Design (Third Edition). Addison-Wesley, 2001.
16. Davidson, S.B., Garcia-Molina, H., Skeen, D. Consistency in Partitioned Networks. ACM Computing Surveys 17(3), September, 1985.
17. Ellis, C.S. The Case for Higher-Level Power Management. In The 7th IEEE Workshop on Hot Topics in Operating Systems. Rio Rico, AZ, March, 1999

[18] Remya, R. R., Samrot, A. V., Kumar, S. S., Mohanavel, V., Karthick, A., Chinnaiyan, V. K., ... &Muhibbullah, M. (2022). Bioactive Potential of Brown Algae. Adsorption Science & Technology, 2022.
[19] Remya, R. R., Julius, A., Suman, T. Y., Mohanavel, V., Karthick, A., Pazhanimuthu, C., ... &Muhibbullah, M. (2022). Role of Nanoparticles in Biodegradation and Their Importance in Environmental and Biomedical Applications. Journal of Nanomaterials, 2022.
[20] Madavan, R., Saroja, S., Karthick, A., Murugesan, S., Mohanavel, V., Velmurugan, P., ... & Sivakumar, S. (2022). Performance analysis of mixed vegetable oil as an alternative for transformer insulation oil. Biomass Conversion and Biorefinery, 1-6.
[21] Mohanavel, V., Ravichandran, M., Anandakrishnan, V., Pramanik, A., Meignanamoorthy, M., Karthick, A., &Muhibbullah, M. (2021). Mechanical properties of titanium diboride particles reinforced aluminum alloy matrix composites: a comprehensive review. Advances in Materials Science and Engineering, 2021.
[22] Raja, T., Ravi, S., Karthick, A., Afzal, A., Saleh, B., Arunkumar, M., ... & Prasath, S. (2021). Comparative Study of Mechanical Properties and Thermal Stability on Banyan/Ramie Fiber-Reinforced Hybrid Polymer Composite. Advances in Materials Science and Engineering, 2021.
[23] Gurusamy, P., Sathish, T., Mohanavel, V., Karthick, A., Ravichandran, M., Nasif, O., ... & Prasath, S. (2021). Finite element analysis of temperature distribution and stress behavior of squeeze pressure composites. Advances in Materials Science and Engineering, 2021.
[24] Dharmaraj, R., Karthick, A., Arunvivek, G. K., Gopikumar, S., Mohanavel, V., Ravichandran, M., & Bharani, M. (2021). Novel approach to handling microfiber-rich dye effluent for sustainable water conservation. Advances in Civil Engineering, 2021.
[25] Aravindh, M., Sathish, S., Prabhu, L., Raj, R. R., Bharani, M., Patil, P. P., ... &Luque, R. (2022). Effect of various factors on plant fibre-reinforced composites with nanofillers and its industrial applications: a critical review. Journal of Nanomaterials, 2022.
[26] Uthirasamy, R., Chinnaiyan, V. K., Vishnukumar, S., Karthick, A., Mohanavel, V., Subramaniam, U., &Muhibbullah, M. (2022). Design of boosted multilevel DC-DC converter for solar photovoltaic system. International Journal of Photoenergy, 2022.
[27] Chandrika, V. S., Thalib, M. M., Karthick, A., Sathyamurthy, R., Manokar, A. M., Subramaniam, U., & Stalin, B. (2021). Performance assessment of free standing and building integrated grid connected photovoltaic system for southern part of India. Building Services Engineering Research and Technology, 42(2), 237-248.