Enhanced Security Model for Pervasive Computing Using Machine Learning Techniques

Jayashree Agarkhed [1] Geetha Pawar [1,2,*]

[1] *Department of Computer Science and Engineering, PDA College of Engineering, Kalaburagi, India.*
[2] *Rajiv Gandhi Institute of technology, Bangalore, India*
[*]*Corresponding author. Email:* geethapawarpda2015@gmail.com

ABSTRACT

In recent mobile world the pervasive computing plays the vital role in data computing and communication. The pervasive computing provides the mobile environment for decentralized computational services where the user work and socializes. Pervasive computing in recent trend moves away from the desktop to make surrounding as flexible and portable dev ices like laptop, notepad, smartphones and personal digital assistants. Pervasive environment devices are worldwide and able to receive various communication services including TV, cable network, radio station and other audio-visual services. The users and the system in this pervasive environment may face the challenges of user trust, data privacy and user and device node identity. To give the feasible determination for these challenges. This paper aims to propose a dynamic-learning pervasive computing environment to refer the challenges' proposed efficient trust model (ETM) for trustworthy and untrustworthy attackers. ETM model also compared with existing generic models, it also provides 97 % accuracy rate than existing models.

Keywords: *ubiquitous computing(ubicomp), pervasive computing, artificial intelligence, machine learning, Enhanced Trust model Introduction.*

1. INTRODUCTION

In recent information technology the world has shifted from desktop computers to easily accessible and smart smaller devices which provide the multiple computation any time anywhere and various types of data communication takes place. In computer era Weiser [1] introduced this most important system of distributed computational service of any-where any-time as pervasive and/or ubiquitous-computing which is the user's day to day practice of using computer. This automated environment of Ubiquitous and pervasive computing focuses on overcoming various imitations of digital world and offered the huge number of advantages such as providing anytime anywhere services making human lifestyle more comfortable in the internet of things and with mobility of users and devices accomplished by providing request to the user as in Fig. 1. The pervasive and ubiquitous computing led to some security issues which have become the challenge for researches. User-nodes and device-nodes inside this dynamic pervasive environment are working together and unknown to each other while operating in this system. The pervasive devices-nodes are performing mutually interacting to each other for computation request and response without knowing each other nodes in prior.

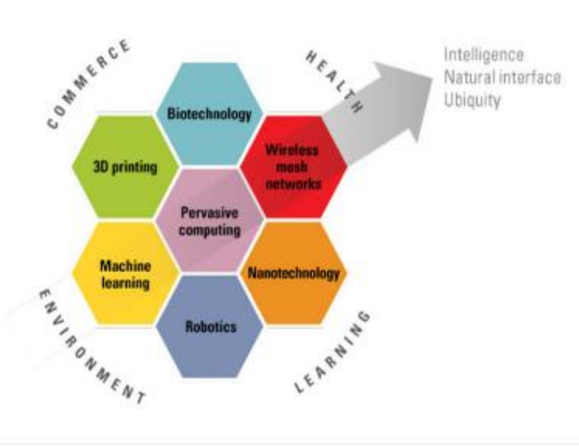


Figure 1 Smart natural interface ubiquity.

Ubiquitous computing [2] networks diverse population of devices and autonomous operation is essential due to absence of central control. In [3] Building the infrastructure of such environment is very dynamic and uncertain. Entities have to deal with the unknown circumstances and also dealing with unexpected interactions to disconnected operation and also has incomplete information about such environment [4].one of the sub concepts of artificial intelligence is the machine learning. The machine learning is to interpret the large data given as input and give the output the knowledge extracted from that large data by the means of different algorithm. machine learning learns the data generate certain rules and estimating the accuracy of such rules the classification of data can be done and specific data can be categorized as trusted and untrusted nodes in the pervasive and ubiquitous computing field. As machine learning is a very scalable model to analyses the data dynamically and put the result in the form of accuracy, recall and support of the interaction of the unknown nodes in this pervasive and ubiquitous environment.

The paper consists of, review on related papers in Section-2, the major challenges of pervasive computing covered in section-3. Proposed ETM model section-4 briefs about the method. Proposed work and evaluation matrixes presented in section 5. Section-6 shows Result Analysis of ETM.

2. RELATED WORK

Development and enhancement embedded system like sensors, networking and computing which again took the attention of pervasive computing, which offers the decentralized computational services. The importance of implementing such environments such as, moving interaction with computers out of a person’s central focus and into the user’s peripheral attention where they can be used subconsciously [5]. Other major focus of pervasive comp system is which make human day to day life easier by giving device-node portability and a smart computation environment that provided requested services to people in the network, when and where they need them [6]. In such environment users of devices have connections with number of smart devices and adopt to the different hardware specification, formats or the software restrictions. Meanwhile there are some security connected risks and also challenges. Which were not encountered in past computing environments.

3. MAJOR CHALLENGES OF PERVASIVE COMPUTING

The major challenges of pervasive computing and are highlighted as follows [7]. Pricing and QoS, Scalability, Heterogeneity, Resource management and load balancing, Adaptability and fault tolerance, Integration. The challenges in subject to privacy, trustworthy and untrustworthy of users and systems and identity become a major research area to such architectures. Scalable and trusted pervasive network demands to efficiently and trustfully identify the user-nodes who uses the environment’s resources [8]. To know the issues and challenges come across during establishment and authenticating the identity of users in such environments. Data privacy in such system is particularly important which leads to be protective of the users’ data [8]. Finding trust relationship among the user and device into such system and computing the recommendation for trust is the major challenge in comparison to traditional authentication [9]. In pervasive field it is difficult to define the limitations of trustworthy environment, which plays vital role when defining trust relationship. Trust also plays a vital role when user-nodes often goes out of such extremities and where generic authentication procedures may not be sufficient [10]. Existing security system has the traditional approaches where the ubiquitous computing demands the new security requirements, in the realm of trusting devices/users. In comparison with human-like decision where trust is evaluated on recommendation when there is less information and priority is set on percentage of previous true information found. Trust evaluated in one domain cannot be same at another domain in ubicomp. Therefore, context understanding is necessary [11]. The state-of-the art in trust management is to represent recommendations and trust propagation through use of certificates [12]. Central authority plays a key role in choosing trusted entities. This view fails to represent many complexities of trust as perceived by humans [13]. For further security enhancement, a Enhance trust model is proposed for pervasive computing using reliable algorithms. The main aim of proposed Enhance trust model is to make network as secure and shows enhancement in terms of accuracy, processing time, precision, recall, f1-score and support.

4. PROPOSED ETM MODEL

The proposed work is to develop an Enhanced trust model to ensure the security issues such as node trust, data-privacy, and device-authenticity over the Internet. To address the problem of retention in back-propagation algorithm, a modified version of the back-propagation Enhanced trust model (ETM) model is used. High accuracy rate for the ETM-based recognition model reflects the application of the proposed model for the considered issue. The proposed model makes use of recommenders at the first interaction for users without historical data. The trust made is based on recommendations gotten from trusted third entities. The proposed model is also developed for recognizing the unfair recommenders.:

Only partial information may be available in the environment, as requests can come from unknown entities or environments may be unfamiliar or hostile.

User entities are likely to become disconnected from their home network and must be able to make fully autonomous security decisions without depending on a specific security infrastructure.

The evolution of trust, which are central to user intuition of the phenomenon, are neglected and are not considered in current systems of environment.

In pervasive and ubicomp environment the present technique is not satisfactory. Therefore, the proposed ETM ubicomp system considers an attribute which are not known previously for service allocator. Thus, this system allows context consideration from where service is called. Table 1 gives the State-of-art-of trust models. In day-to-day life pervasive and ubiquitous computing provides many services like communication, storage request computation which appears anytime anywhere, which needs heterogeneous resource integration and enhanced and scalable environment where smart mobile devices and powerful cloud platform existing [25-28].

5. PROPOSED WORK AND EVALUATION MATRIX

The main contributions of proposed ETM model are as follows:

In enhanced trust model, an AI technique is proposed to fetch the communication between the user in the network.

Back propagation classification algorithm taken to compute the trust and it solves the problems involving simultaneous interdependent decision and estimation in classification issues [29-32].

The enhanced trust model results show the use of such method and solving the issues of existing system.

The back propagation algorithm has been used for the classification of trusted and untrusted users with a dataset of 300 transactions and 5 features. During pre-processing, the data cleaning is performed and correct dataset is considered to avoid overfitting.

A hold-out method has been used for testing and training of the models. The applicability of the proposed algorithm is also tested using this ETM model. Additional performance evaluation metrices such as accuracy, processing time, precision, recall, f1-score and support computed for model's performance evaluations. Build the model using different algorithms Decision tree, Random Forest classifier, SVM, Gaussian NB, MLP classifier.

Back propagation algorithm gives good performance as in comparison with other classification algorithm. The back-propagation algorithm learnings the weight and iterates on less and less error is good in sequence learning but fails in taking more epochs. This ETM model provided efficient results for many machine learning problems such as text-identification, speech recognition, trusted and untrusted detection problems, and many others. Improved accuracy: ETM model does a prediction with much better accuracy than the existing systems. Comparison graph of the existing model and proposed model shows the extent of accuracy improvement.

Time efficiency is improved which is the most important criteria when it comes to mass data and lesser availability of raw computation power with the advancement of time. Less resource requirement: The resource requirement, that is, the hardware and the software needed to achieve this is very less. A fast, accurate result can be generated in very less time. Recurrent neural networks are capable of learning and as number of epochs increases the accuracy also improves. It can dramatically speed up the learning process. Intrusion detection model: In this environment untrusted node detection at the objective node to activate a firewall and to alert host devices-node when an authorized access or unauthorized traffic is detected. ETM-based classification model: This model provided prominent results for many machine learning problems in embedded with natural language processing like syntactically analyzing the text recognition, speech processing, wireless mesh network attack detection problems, and many others.

Table 1. State-of-art-of-trust models

Reference	Model	Algorithm used	Methodology	Accuracy	Future work
He *et al.* [14]-2020	Long short-term memory (LSTM)Model	Back-Propagation Deep Neural Network	At the -pervasive development of trusted model, the deep-learning-based pervasive architecture is used for the considered security issues	93.87%	To find out the unfair recommender of the node in the dynamic accessing environment.
Irfan Uddin *et al.* [15]	single-layer neural network (NN), five-layer DNN	logistic regression, SVM, and Na¨ıve Bayes	NN and DNN-based machine learning model used with classification algorithm to know the attackers' activities	95%	To predicting the behaviors of terrorist activities
Ali Shah *et al.*[16]	Deep learning-based model	Neural-network algorithm	This model considered the parameter of employee selection and apply the	90.6%	Further looking to take necessary action for absenteeism pattern of staff using association rules

		And deep learning algorithm	model to take decision on absenteeism pattern of staff		
D’Angelo *et al.*[17]	An Effective trust model	Apriori algorithm, naïve bayes classifier	The algorithm searches the user’s pattern of communicating with each other and classifier specifies the trusted and untrusted users	More than 95% based on number of transactions	Finding out the false recommendation
Kurniawan and Kyas [18]	TrustBayes model	Bayesian decision theory	The model provides access control in uncertainty field of communication	on lesser nodes trust is nearly 60%	Getting prior knowledge of environment and behaviors of node
Dangelo *et al.* [19]	Trust model	Association rules, naïve bayes classifier	Model use human like decision making on trusting the user and devices in pervasive environment	92%	By adding on new attributes proposed model working on portable devices in real-world-scenarios
Zhang *et al.* [20]	CNN-based-model	Deep-learning algorithm	Model is used to detect the specific colour fish in the real-world system	-	Automatic object tracking
Yu *et al.* [21]	Weight-optimization model and voting-strategy model	Classifier algorithm	Classify human action and back-ground information in nonsequential network-topology	-	To learn the nonsequential environment
Kraounakis *et al.*[22]	DCR-based computational model	Classifier algorithm	Classifies the inaccurate ratings	-	Unfair feedback rating
Yan and Wang[23]	General trust and local trust	-	Attribute based encryption on pervasive social networking nodes	-	High performance encryption and decryption techniques
Sharma *et al.* [24]	Flexible mixture model (FMM)	-	Generate high trust values within the users with low cost of monitoring	-	Predicting user rating with low-cost error

Improved Processing time: ETM
Guard at the objective node to activate a firewall.

Alert the users.

Keras sequential API to build the model.

Activation function is “relu”

Activation function for last dense layer is “Softmax”

Optimizer: SGD

Serialize the model by saving with json notation.

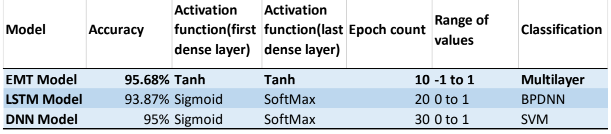
Train and evaluate the model

Back-propagation Classification Module: Convert the categorial data set into numerical data and build the model using different algorithms Decision tree, Random Forest classifier, SVM, Gaussian NB, MLP classifier.

Train & Test all the models.

Improved accuracy: ETM model does a prediction with much better accuracy than the existing systems. Comparison graph of the existing model and proposed model shows the extent of accuracy improvement. Time efficiency is improved which is the most important criteria when it comes to mass data and lesser availability of raw computation power with the advancement of time.

Less resource requirement: The resource requirement, i.e., the hardware and the software needed to achieve this is very less. A fast, accurate result can be generated in very less time. Enhanced Trusted Model: the back propagation algorithm helps in having many epochs and get better accuracy over the weight and reduction in error. Improved Processing time: ETM recurrent neural networks are capable of learning and remembering over long sequences of inputs. It can dramatically speed up the learning process based on epochs [33-38].



Model	Accuracy	Activation function(first dense layer)	Activation function(last dense layer)	Epoch count	Range of values	Classification
EMT Model	**95.68%**	**Tanh**	**Tanh**	**10**	**-1 to 1**	**Multilayer**
LSTM Model	93.87%	Sigmoid	SoftMax	20	0 to 1	BPDNN
DNN Model	95%	Sigmoid	SoftMax	30	0 to 1	SVM

Figure 2 Performance comparison

In Fig. 3 the ETM model built, first import the dataset from UCI machine learning repository. We can also generate our own custom data, or the data can be taken from then interaction. The data collected if transformed and normalized as per requirement for building the model. The data is pre-processed because data will be in different ranges. We must normalize it between -1 and 1 because machine can process only between that range as we make use of tanh function. We remove fields which are not required and remove null values. Then the ETM model is built using Keras which works on TensorFlow. After the model is built, we must train the model on train dataset and test the model on test dataset. The model is compiled to specify the required parameters and evaluated to get the expected accuracy.

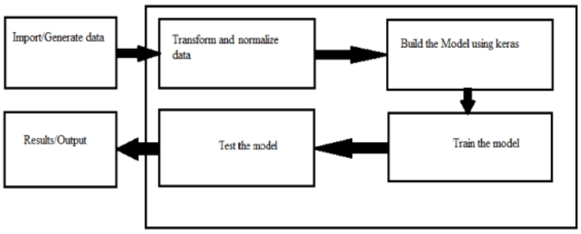


Figure 3 ETM data building process

6. RESULT ANALYSIS OF ETM MODEL

The back propagation algorithm has been used for the classification of trusted and untrusted users with a dataset of 300 transactions and 5 features. During pre-processing, the data cleaning is performed and correct dataset is maintained.

In Fig:4 the categories of attacks considered in the pervasive environment the Categorize are normal, U2R attack, R2L attack, Probe attack, DoS attack.

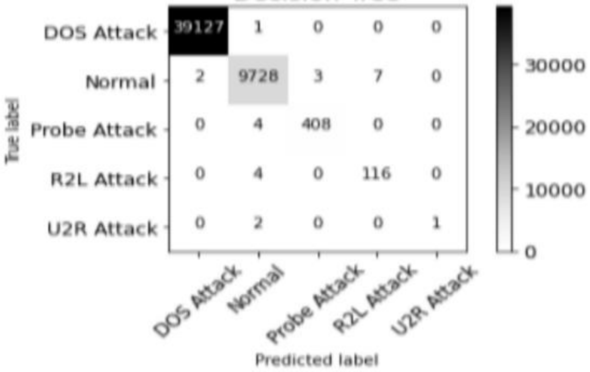


Figure 4 categories of attacks

As analysed in the figure 5 the training accuracy and the validation accuracy increases as the number of iterations increases in comparison with other models.

ETM works well over a broad range of parameters such as learning rate, input gate bias and output gate bias.

• For long time lag problems ETM can handle noise, distributed representations, and continuous values

• The performance results of the ETM-based model it generates an accuracy rate of 95.68%

• They are able to model long-term sequence dependencies

• ETM gives us the most Control-ability and thus, Better Results

Figure:4 training accuracy and validation accuracy at 30 epochs

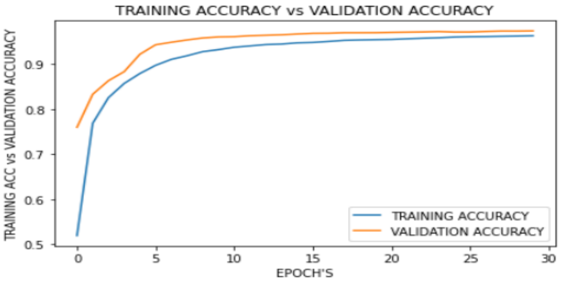
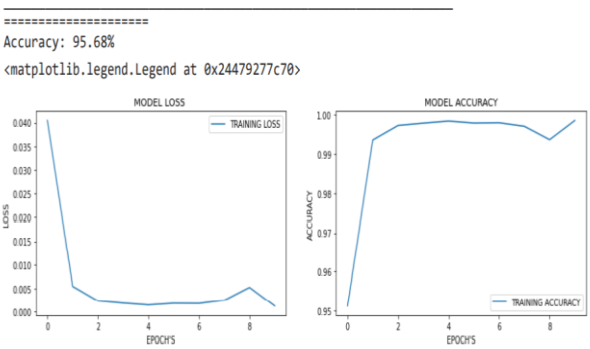


Figure 5 Comparison of Accuracy

Fig. 5 shows the ETL models' limitation is very low as the epochs increases and model's accuracy is increasing as the epochs increases.



```
======================
Accuracy: 95.68%
<matplotlib.legend.Legend at 0x24479277c70>
```

Figure 6 Loss and accuracy comparison on epochs

Figure 2 shows the comparison on parameters like accuracy, activation function at first dense layer, activation function at last dense layer, epoch count, range of values, and classification.

7. CONCLUSION

Enhancement of security in pervasive and ubiquitous computing environment improves user experience seamlessly. The proposed ETM model enhances the security in the network and demonstrated a significant performance improvement with an accuracy rate of 97%.

REFERENCES

[1] M. Weiser, "*e computer for the 21st century," Mobile Computing and Communications Review, vol. 3, pp. 3–11, 1999

[2] C. da Costa, A. Yamin and C. Geyer, "Toward a General Software Infrastructure for Ubiquitous Computing", IEEE Pervasive Computing, vol. 7, no. 1, pp. 64-73, 2008

[3] H. Rashvand, V. Traver Salcedo, E. Montón Sánchez and D. Iliescu, "Ubiquitous wireless telemedicine", IET Communications, vol. 2, no. 2, p. 237, 2008Author, F., Author, S., Author, T.: Book

[4] M. Haque and S. Ahamed, "An Impregnable Lightweight Device Discovery (ILDD) Model for the Pervasive Computing Environment of Enterprise Applications", IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 38, no. 3, pp. 334-346, 2008.

[5] K. Park, U. Yoon and S. Kim, "Personalized Service Discovery in Ubiquitous Computing Environments", IEEE Pervasive Computing, vol. 8, no. 1, pp. 58-65, 2009.

[6] W. Chang, T. Wang, F. Lin and H. Yang, "Game-Based Learning with Ubiquitous Technologies", IEEE Internet Computing, vol. 13, no. 4, pp. 26-33, 2009.

[7] R. Wang, Y. Chang and R. Chang, "Design Issues of Semantic Service Discovery for Ubiquitous Computing", 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE'07), 2007.

[8] T. Kaur and J. Singh, "Security Issues in Design and Development of High Performance Ubiquitous Computing", 2014 International Conference on Computational Intelligence and Communication Networks, 2014.

[9] N. Kato, S. Guo and V. Misic, "Guest Editorial: Special Issue of IEEE Transactions on Emerging Topics in Computing on Emerging Mobile and Ubiquitous Systems Part—II", IEEE Transactions on Emerging Topics in Computing, vol. 3, no. 3, pp. 305-306, 2015.

[10] C. Graves, T. Negron, M. Chestnut II and G. Popoola, "Studying Smart Spaces Using an "Embiquitous" Computing Analogy", IEEE Pervasive Computing, vol. 14, no. 2, pp. 64-68, 2015.

[11] G. DAngelo, S. Rampone and F. Palmieri, "An Artificial Intelligence-Based Trust Model for Pervasive Computing", 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015.

[12] C. Fernandez Campusano, R. Cortinas Rodriguez and M. Larrea Alava, "Boosting Dependable Ubiquitous Computing: A Case Study", IEEE Latin America Transactions, vol. 12, no. 3, pp. 442-448, 2014.

[13] C. Lee, Gyu Myoung Lee and Woo Seop Rhee, "Standardization and challenges of smart ubiquitous networks in ITU-T", IEEE Communications Magazine, vol. 51, no. 10, pp. 102-110, 2013.

[14] Yang He, Shah Nazir, Baisheng Nie,Sulaiman Khan , Jianhui Zhang" Developing an Efficient Deep Learning-Based Trusted Model for Pervasive Computing Using an LSTM-Based Classification Model" Volume 2020, Article ID 4579495, 6 pages.

[15] M. I. Uddin, N. Zada, F. Aziz et al., "Prediction of future terrorist activities using deep neural networks," Complexity, vol. 2020, 16 pages, 2020.

[16] S. A. Ali Shah, I. Uddin, F. Aziz, S. Ahmad, M. A. Al-Khasawneh, and M. Sharaf, "An enhanced deep neural network for predicting workplace absenteeism," Complexity, vol. 2020, 12 pages, 2020.

[17] G. D'Angelo, S. Rampone and F. Palmieri, "Developing a trust model for pervasive computing based on Apriori association rules learning and Bayesian classification", Soft Computing, vol. 21, no. 21, pp. 6297-6315, 2016.

[18] A. Kurniawan and M. Kyas, "A trust model-based Bayesian decision theory in large scale Internet of things," in Proceedings of the 2015 IEEE

[19] Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Singapore, Singapore, pp. 1–5, April 2015.

[20] G. Dangelo, S. Rampone, and F. Palmieri, "An artificial intelligence-based trust model for pervasive computing," in Proceedings of the 2015 10th international conference on P2p, parallel, grid, cloud and internet computing (3pgcic), pp. 701–706, Krakow, Poland, November 2015.

[21] L. Zhang, C. P. Lim, and J. Han, "Complex deep learning and evolutionary computing models in computer vision," Complexity, vol. 2019, Article ID 1671340, 2019.

[22] X. Yu, Z. Zhang, L. Wu et al., "Deep ensemble learning for human action recognition in still images," Complexity, vol. 2020, Article ID 9428612, 2020.

[23] S. Kraounakis, I. Demetropoulos, A. Michalas, M. Obaidat, P. Sarigiannidis and M. Louta, "A Robust Reputation-Based Computational Model for Trust Establishment in Pervasive Systems", IEEE Systems Journal, vol. 9, no. 3, pp. 878-891, 2015.

[24] Z. Yan and M. Wang, "Protect Pervasive Social Networking Based on Two-Dimensional Trust Levels", IEEE Systems Journal, vol. 11, no. 1, pp. 207-218, 2017.

[25] V. Sharma, I. You, R. Kumar and P. Kim, "Computational Offloading for Efficient Trust Management in Pervasive Online Social Networks Using Osmotic Computing", IEEE Access, vol. 5, pp. 5084-5103, 2017.

[26] Bhuvaneswary, N., S. Prabu, S. Karthikeyan, R. Kathirvel, and T. Saraswathi. "Low Power Reversible Parallel and Serial Binary Adder/Subtractor." Further Advances in Internet of Things in Biomedical and Cyber Physical Systems (2021): 151.

[27] Le, Ngoc Tuyen, Jing-Wein Wang, Duc Huy Le, Chih-Chiang Wang, and Tu N. Nguyen. "Fingerprint enhancement based on tensor of wavelet subbands for classification." IEEE Access 8 (2020): 6602-6615.

[28] Naeem, Muhammad Ali, Tu N. Nguyen, Rashid Ali, Korhan Cengiz, Yahui Meng, and Tahir Khurshaid. "Hybrid Cache Management in IoT-based Named Data Networking." IEEE Internet of Things Journal (2021).

[29] Prabu, S., Balamurugan Velan, F. V. Jayasudha, P. Visu, and K. Janarthanan. "Mobile technologies for contact tracing and prevention of COVID-19 positive cases: a cross-sectional study." International Journal of Pervasive Computing and Communications (2020).

[30] Hu, Liwen, Ngoc-Tu Nguyen, Wenjin Tao, Ming C. Leu, Xiaoqing Frank Liu, Md Rakib Shahriar, and SM Nahian Al Sunny. "Modeling of cloud-based digital twins for smart manufacturing with MT connect." Procedia manufacturing 26 (2018): 1193-1203.

[31] Subramani, Prabu, K. Srinivas, R. Sujatha, and B. D. Parameshachari. "Prediction of muscular paralysis disease based on hybrid feature extraction with machine learning technique for COVID-19 and post-COVID-19 patients." Personal and Ubiquitous Computing (2021): 1-14.

[32] Kumar, M. Keerthi, B. D. Parameshachari, S. Prabu, and Silvia liberata Ullo. "Comparative Analysis to Identify Efficient Technique for Interfacing BCI System." In IOP Conference Series: Materials Science and Engineering, vol. 925, no. 1, p. 012062. IOP Publishing, 2020.

[33] Rajendrakumar, Shiny, and V. K. Parvati. "Automation of irrigation system through embedded computing technology." In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, pp. 289-293. 2019.

[34] Z. Guo, L. Tang, T. Guo, K. Yu, M. Alazab, A. Shalaginov, “Deep Graph Neural Network-based Spammer Detection Under the Perspective of Heterogeneous Cyberspace”, Future Generation Computer Systems, https://doi.org/10.1016/j.future.2020.11.028.

[35] Y. Sun, J. Liu, K. Yu, M. Alazab, K. Lin, “PMRSS: Privacy-preserving Medical Record Searching Scheme for Intelligent Diagnosis in IoT Healthcare”, IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2021.3070544.

[36] N. Shi, L. Tan, W. Li, X. Qi, K. Yu, “A Blockchain-Empowered AAA Scheme in the Large-Scale HetNet”, Digital Communications and Networks, https://doi.org/10.1016/j.dcan.2020.10.002.

[37] C. Feng et al., "Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach," IEEE Network, vol. 35, no. 1, pp. 130-137, January/February 2021, doi: 10.1109/MNET.011.2000223.

[38] L. Tan, H. Xiao, K. Yu, M. Aloqaily, Y. Jararweh, “A Blockchain-empowered Crowdsourcing System for 5G-enabled Smart Cities”, Computer Standards & Interfaces, https://doi.org/10.1016/j.csi.2021.103517

[39] K. Yu, L. Tan, X. Shang, J. Huang, G. Srivastava and P. Chatterjee, “Efficient and Privacy-Preserving Medical Research Support Platform Against COVID-19: A Blockchain-Based Approach”, IEEE Consumer Electronics Magazine, doi: 10.1109/MCE.2020.3035520.