
Jayashree Agarkhed¹ Geetha Pawar¹,²,*

¹Department of Computer Science and Engineering, PDA College of Engineering, Kalaburagi, India.
²Rajiv Gandhi Institute of Technology, Bangalore, India
*Corresponding author. Email: geethapawarpa2015@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 devices 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. Users-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 systm 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 PERVERSIVE 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 metrics 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>
<thead>
<tr>
<th>Reference</th>
<th>Model</th>
<th>Algorithm used</th>
<th>Methodology</th>
<th>Accuracy</th>
<th>Future work</th>
</tr>
</thead>
<tbody>
<tr>
<td>He et al. [14]-2020</td>
<td>Long short-term memory (LSTM)Model</td>
<td>Back-Propagation Deep Neural Network</td>
<td>At the -pervasive development of trusted model, the deep-learning-based pervasive architecture is used for the considered security issues</td>
<td>93.87%</td>
<td>To find out the unfair recommender of the node in the dynamic accessing environment.</td>
</tr>
<tr>
<td>Irfan Uddin et al. [15]</td>
<td>single-layer neural network (NN), five-layer DNN</td>
<td>logistic regression, SVM, and Naïve Bayes</td>
<td>NN and DNN-based machine learning model used with classification algorithm to know the attackers’ activities</td>
<td>95%</td>
<td>To predicting the behaviors of terrorist activities</td>
</tr>
<tr>
<td>Ali Shah et al.[16]</td>
<td>Deep learning-based model</td>
<td>Neural-network algorithm</td>
<td>This model considered the parameter of employee selection and apply the</td>
<td>90.6%</td>
<td>Further looking to take necessary action for absenteeism pattern of staff using association rules</td>
</tr>
</tbody>
</table>
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].

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.

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.

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.

- 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

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

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


