International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

Bond Decision of Arrangement Classifiers under Violation

MR. P. MAHIPAL REDDY [1] & MS. G. MANIMITHRA [2]

[1]Assistant Professor Department of CSE Vaagdevi Engineering College, Bollikunta, Warangal, and Telangana State, India.

[2]M-Tech Computer Science & Engineering Department of CSE Vaagdevi Engineering College, Bollikunta, Warangal, and Telangana State, India.

Abstract: Sample category systems are typically used in adverse programs, like biometric authentication, network intrusion detection, and unsolicited mail filtering, in which records may be purposely manipulated through humans to undermine their operation. As this adversarial state of affairs isn't always taken into consideration via classical design strategies, pattern class systems might also exhibit vulnerabilities, whose exploitation might also severely have an effect on their overall performance, and therefore restrict their realistic software. Extending sample category idea and layout strategies to adverse settings is consequently a singular and really applicable studies course, which has now not yet been pursued in a systematic way. in this paper, we cope with one of the main open issues: evaluating at layout section the security of sample classifiers, namely, the performance degradation underneath potential assaults they'll incur during operation. We advise a framework for empirical assessment of classifier security that formalizes and generalizes the principle thoughts proposed in the literature, and provide examples of its use in three actual packages. said results show that protection assessment can offer a extra whole expertise of the classifier's behavior in adversarial environments, and lead to better design picks.

Index phrases—pattern category, adverse class, overall performance assessment, protection evaluation, robustness assessment

1 Advent

Sample category systems primarily based on device getting to know algorithms are generally utilized in protection-associated applications like biometric authentication, network intrusion detection, and spam filtering, to discriminate between a "valid" and a "malicious" pattern elegance (e.g., valid and spam emails). contrary to traditional ones, those applications have an intrinsic adversarial nature for the reason that input data may be purposely manipulated via an sensible and adaptive adversary to undermine classifier operation. This often gives rise to an hands race among the adversary and the classifier dressmaker. Well known examples of attacks towards pattern classifiers are: submitting a faux biometric trait to a biometric authentication machine (spoofing assault)

editing community packets belonging to intrusive visitors to stay away from intrusion detection systems (IDSs) manipulating the content of junk mail emails to get them past spam filters (e.g., by misspelling commonplace unsolicited mail words to keep away from their detection). Adversarial eventualities also can arise in smart facts evaluation and information retrieval; e.g., a malicious webmaster may additionally manipulate search engine rankings to artificially sell her1 website. It is now acknowledged that, considering the fact that sample class structures based totally on classical concept and design techniques [9] do no longer keep in mind hostile settings, they show off vulnerabilities to numerous ability attacks, allowing adversaries to undermine their effectiveness. A systematic and unified treatment of this problem is as a result needed to permit the relied on adoption of pattern classifiers in opposed environments, beginning from the theoretical foundations up to novel design methods, extending the classical design cycle. in particular, 3 principal open issues may be recognized: (i) reading the vulnerabilities of classification algorithms, and the corresponding attacks; (ii) developing novel strategies to evaluate classifier security in opposition to those assaults, which isn't feasible using classical overall performance assessment strategies; (iii) developing novel design techniques to guarantee classifier security in opposed environments.

2 Background and previous paintings:

Here we overview preceding paintings, highlighting the concepts with the intention to be exploited in our framework.

2.1Taxonomy of attacks in opposition to sample Classifiers

Taxonomy of potential attacks against sample classifiers was proposed and eventually extended. we can take advantage of it in our framework, as part of the definition of assault eventualities. The taxonomy is based on two important capabilities: the sort of impact of assaults on the classifier, and the kind of safety violation they purpose. The affect may be both causative, if it undermines the gaining knowledge of algorithm to cause subsequent misclassifications; or exploratory, if it exploits information of the skilled classifier to cause misclassifications, without affecting the getting to know algorithm. Therefore, causative attacks may also have an effect on both training and trying out records, or handiest training facts, whereas exploratory assaults have an effect on handiest testing records. the security violation may be an integrity violation, if it lets in the adversary to get admission to the provider or resource covered by way of the classifier; an availability violation, if it denies legitimate users access to it; or a privacy violation, if it permits the adversary to attain personal records from the classifier. Integrity violations bring about misclassifying malicious samples as legitimate, at the same time as availability violations can also reason valid samples to be misclassified as malicious. a 3rd feature of the taxonomy is the specificity of an attack, that degrees from focused to indiscriminate, relying on whether the assault focuses on a single or few particular samples (e.g., a particular spam email misclassified as legitimate), or on a wider set of samples.

2.2 limitations of Classical performance evaluation methods in opposed type

Classical performance assessment techniques, like ok-fold move validation and bootstrapping, goal to estimate the performance that a classifier

will exhibit for the duration of operation, by the usage of statistics D accrued for the duration of classifier design.2 those methods are primarily based on the stationarity assumption that the information visible at some stage in operation comply with the equal distribution as D. accordingly, they resample D to construct one or extra pairs of education and testing sets that ideally comply with the identical distribution as D [9]. however, the presence of an shrewd and adaptive adversary makes the classification problem especially non-desk bound, and makes it tough to predict how many and which varieties of attacks a classifier will be problem to for the duration of operation, this is, how the information distribution will exchange. in particular, the testing statistics processed by way of the skilled classifier can be laid low with both exploratory and causative assaults, whilst the schooling statistics can best be laid low with causative attacks, if the classifier is retrained on-line. In each case, during operation, trying out information may additionally comply with a special distribution than that of training statistics, while the classifier is underneath assault. Consequently, security assessment cannot be carried out in step with the classical paradigm of performance assessment 4.

2.3 Hands Race and safety by using design

Safety issues frequently cause a "reactive" hands race between the adversary and the classifier fashion designer. At each step, the adversary analyzes the classifier defenses, and develops an assault strategy to overcome them. The clothier reacts by way of reading the radical assault samples, and, if required, updates the classifier; normally, by using retraining it on the brand new amassed samples, and/or including features which could detect the radical assaults (see Fig. 1, left). Examples of this arms race can be determined in junk mail filtering and malware detection, where it has led to a good sized growth within the variability and class of assaults and countermeasures. To at ease a gadget, a not unusual approach used in engineering and cryptography is security by way of obscurity that is based on keeping mystery some of the device information to the adversary. In evaluation, the paradigm of security with the aid of layout advocates that systems must be designed from the ground-up to be comfortable, without assuming that the adversary might also ever discover some critical gadget information.

The purpose of safety assessment is to deal with issue (i) above, i.e., to simulate a number of sensible attack situations that can be incurred for the duration of operation, and to assess the impact of the corresponding attacks at the targeted classifier to spotlight the maximum important vulnerabilities. This amounts to acting a what-if evaluation, that's a common exercise in safety. This approach has been implicitly accompanied in several previous works (see segment 2.4), but never formalized within a widespread framework for the empirical assessment of classifier security. Although protection evaluation may additionally suggest specific countermeasures, the layout of relaxed classifiers, i.e., trouble (ii) above, stays a distinct open problem.

2.4 preceding work on safety assessment

Many authors implicitly done safety assessment as a what-if analysis, based on empirical simulation strategies; but, they mainly targeted on a particular utility, classifier and attack, and devised ad hoc protection assessment tactics primarily based on the exploitation of hassle information and heuristic techniques. Their intention become either to point out a previously unknown vulnerability, or to assess protection

against a recognized assault. In some instances, precise countermeasures were additionally proposed, consistent with a proactive/protection-by-design approach. assaults were simulated by means of manipulating schooling and trying out samples in keeping with software-precise criteria most effective, without reference to greater standard hints; consequently, such strategies can't be without delay exploited with the aid of a machine designer in greater trendy instances. a few works proposed analytical techniques to assess the safety of getting to know algorithms or of some training of choice features (e.g., linear ones), primarily based on greater preferred, utility-independent criteria to model the adversary's behavior (inclusive of percent getting to know and recreation principle). Some of these standards might be exploited in our framework for empirical security evaluation; specially, in the definition of the adversary version defined in phase 3.1, as high-stage pointers for simulating attacks.

2.5 Building on preceding work

We summarize here the 3 major ideas extra or much less explicitly emerged from previous paintings in an effort to be exploited in our framework for protection assessment. 1) arms race and protection with the aid of design: because it isn't possible to are expecting how many and which styles of assaults a classifier will incur during operation, classifier security ought to be proactively evaluated the use of a what-if evaluation, through simulating potential assault scenarios. 2) Adversary modeling: powerful simulation of attack situations requires a proper version of the adversary. 3) Information distribution beneath assault: the distribution of trying out statistics might also range from that of schooling information, whilst the classifier is underneath assault.

3. A FRAMEWORK FOR EMPIRICAL EVALUATION OF CLASSIFIER PROTECTION

We advise right here a framework for the empirical evaluation of classifier security in antagonistic environments, that unifies and builds on the three concepts highlighted in segment 2.5. Our important goal is to provide a quantitative and popular-motive basis for the application of the what-if evaluation to classifier security assessment, based totally on the definition of potential attack eventualities. To this stop, we propose: (i) a model of the adversary that permits us to outline any assault situation; (ii) a corresponding version of the information distribution; and (iii) a method for producing training and testing sets which might be consultant of the data distribution, and are used for empirical performance assessment.

3.1 assault scenario and version of the Adversary

Even though the definition of attack scenarios is in the end an utility-precise issue, it is viable to give popular tips that can assist the clothier of a sample popularity machine. Right here we advise to specify the assault scenario in terms of a conceptual model of the adversary that encompasses, unifies, and extends distinctive ideas from preceding paintings. Our version is based totally on the idea that the adversary acts rationally to obtain a given aim, according to her understanding of the classifier, and her functionality of manipulating statistics. This permits one to derive the corresponding optimal assault strategy.

Adversary's intention: It is miles formulated as the optimization of an goal function. We advocate to define this function primarily based at the favored protection violation (integrity,

availability, or privacy), and at the attack specificity (from focused to indiscriminate), in keeping with the taxonomy (see segment 2.1). As an example, the goal of an indiscriminate integrity violation can be to maximize the fraction of misclassified malicious samples. The aim of a focused privacy violation can be to obtain a few unique, exclusive facts from the classifier (e.g., the biometric trait of a given user enrolled in a biometric device) by exploiting the magnificence labels assigned to a few "question" samples, at the same time as minimizing the variety of query samples that the adversary has to problem to violate privacy.

Adversary's knowledge: Assumptions on the adversary's know-how have most effective been qualitatively discussed in preceding paintings, specifically relying at the software at hand. Here we advocate a more systematic scheme for their definition, with admire to the expertise of the unmarried components of a pattern classifier: (ok.i) the training information; (ok.ii) the characteristic set; (k.iii) the learning set of rules and the type of choice characteristic (e.g., a linear SVM); (k.iv) the classifier's choice feature and its parameters (e.g., the function weights of a linear classifier); (ok.v) the remarks to be had from the classifier, if any (e.g., the class labels assigned to a few "question" samples that the adversary issues to get remarks. It is miles worth noting that practical and minimum assumptions about what may be saved completely mystery from the adversary have to be achieved. Examples of adversary's understanding are given in section 4.

Adversary's functionality: It refers to the management that the adversary has on education and checking out information. We endorse to outline it in terms of: (c.i) the assault have an impact on (both causative or exploratory), as defined; (c.ii) whether or not and to what quantity the attack impacts the elegance priors; (c.iii) how many and which training and checking out samples can be managed through the adversary in each elegance; (c.iv) which capabilities can be manipulated, and to what volume, taking into account software-specific constraints (e.g., correlated functions cannot be modified independently, and the functionality of malicious samples cannot be compromised).

Attack strategy: Possible finally define the most efficient assault method, particularly, how education and checking out information have to be quantitatively modified to optimize the goal function characterizing the adversary's goal. Such adjustments are described in terms of: (a.i) how the class priors are modified; (a.ii) what fraction of the samples of elegance is affected by the attack; and (a.iii) how capabilities are manipulated via the attack. Detailed examples are given in segment 4. As soon as the attack situation is defined in terms of the adversary model and the resulting assault strategy, our framework proceeds with the definition of the corresponding information distribution, That is used to construct schooling and trying out sets for security assessment.

3.2 A model of the facts Distribution

We don't forget the usual setting for classifier design in a problem which consists of discriminating between valid (L) and malicious (M) samples: a gaining knowledge of algorithm and a performance measure were chosen, a set D of n labelled samples has been collected, and a fixed of d capabilities have been extracted, so that $D = \{(x_i; y_i)\}^n$ I=1, wherein xi denotes a d-dimensional function vector, and yi 2 fL;Mg a category label. The pairs ðxi; yiÞ are assumed to be i.i.d. samples of a few unknown distribution pD (X; Y). Since the adversary model in section

three.1 requires us to specify how the attack impacts the class priors and the features of every elegance, we don't forget the classical generative model pD(X; Y) = pD|(Y) pD(X, Y). To account for the presence of assaults during operation, which may also affect both the training or the testing information, or each, we denote the corresponding education and trying out distributions as ptr and pts, respectively. We will simply write p while we need to refer to both of them, or both, and the that means is apparent from the context. We extend this assumption to the components of ptr and pts that are not laid low with the attack (if any), with the aid of assuming that they continue to be same to the corresponding distribution pD (e.g., if the attack does now not affect the magnificence priors, the above equality additionally holds below attack). The distributions p(Y) and p(X,Y) that are tormented by the attack can be described as follows, consistent with the definition of the assault approach, (a.i-iii).

3.4 A way to Use Our Framework

We summarize right here the steps that the fashion designer of a pattern classifier have to take to evaluate its protection the usage of our framework, for every assault situation of hobby. They extend the overall performance assessment step of the classical design cycle, that's used as a part of the version choice segment, and to assess the very last classifier to be deployed.

1) Assault situation: The attack state of affairs have to be defined at the conceptual degree by way of making unique assumptions on the intention, knowledge (ok.i-v), and functionality of the adversary (c.i-iv), and defining the corresponding attack method (a.iiii), consistent with the model of phase 3.1.

2) facts version. in keeping with the hypothesized assault scenario, the dressmaker have to define the distributions p(Y), p(A|Y), and p(X|Y ;A), for Y 2 fL;Mg, fF;Tg, and for schooling and checking out information.

3) production of TR and TS. Given k

---

1 pairs (Di TR;Di TS), i = 1; . . . ; okay, acquired from classical re-sampling strategies like pass-validation or bootstrapping, the scale of TR and TS need to be described, and algorithm 1 have to be run with the corresponding inputs to reap TRi and TSi. If the assault does not affect the schooling (trying out) records, TRi (TSi) is set to Di TR (Di TS).

4) Overall performance evaluation: The classifier overall performance underneath the simulated attack is evaluated the use of the constructed (TR_i, TS_i) pairs, as in classical techniques.

4 UTILITY EXAMPLES

Even as previous paintings focused on a single application, we remember right here three extraordinary application examples of our framework in unsolicited mail filtering, biometric authentication, and community intrusion detection. Our goal is to show how the clothier of a sample classifier can use our framework, and what kind of additional statistics he can reap from protection evaluation. we are able to display that a tradeoff between classifier accuracy and protection emerges from time to time, and that this facts can be exploited for numerous purposes; e.g., to improve the version selection segment by means of considering each class accuracy and protection.

4.1 junk mail Filtering

Count on that a classifier has to discriminate between legitimate and unsolicited mail emails on the idea of their text, and that the bag-of-phrases function illustration has been selected, with binary functions denoting the occurrence of a given set of phrases. This form of classifier has been taken into consideration by means of several authors and it is covered in numerous actual junk mail filters. In this situation, we have attention on version selection. We expect that the dressmaker wants to choose between a assist vector machine (SVM) with a linear kernel, and a logistic regression (LR) linear classifier. He also desires to choose a characteristic subset, amongst all of the words occurring in training emails.

Attack scenario: Aim. The adversary aims at maximizing the proportion of junk mail emails misclassified as legitimate that is an indiscriminate integrity violation.

Know-how: The adversary is believed to have ideal know-how of the classifier, i.e.,: (ok.ii) the characteristic set, (okay.iii) the form of decision characteristic, and (k.iv) its parameters (the burden assigned to every feature, and the choice threshold). Assumptions at the understanding of (ok.i) the schooling data and (okay.v) remarks from the classifier are now not relevant in this case, as they do not provide any extra records.

Functionality: We expect that the adversary: (c.i) is simplest capable to influence trying out data (exploratory attack); (c.ii) cannot adjust the class priors; (c.iii) can manage every malicious sample, however no valid ones; (c.iv) can control any characteristic fee (i.e., she can insert or obfuscate any phrase), However up to a most number nmax of functions in each unsolicited mail electronic mail. This lets in us to evaluate how gracefully the classifier overall performance degrades as more and more features is modified, via repeating the evaluation for increasing values of n_{max}.

4.2 Biometric Authentication

Multimodal biometric structures for private identity popularity have received incredible hobby inside the beyond few years. It has been proven that combining facts coming from unique biometric traits can conquer the limits and the weaknesses inherent in each character biometric, resulting in a better accuracy. The reason is that, to avoid a multimodal device, one expects that the adversary need to spoof all of the corresponding biometric trends. on this application example, we display how the clothier of a multimodal system can verify if this hypothesis holds, before deploying the gadget, through simulating spoofing assaults towards every of the matchers. To this case, we partly make the most of the evaluation.

We don't forget a regular multimodal machine, made from a fingerprint and a face matcher, which operates as follows. The design segment includes the enrollment of authorized users (customers): reference templates in their biometric developments are saved into a database, together with the corresponding identities. during operation, every user offers the requested biometric developments to the sensors, and claims the identity of a patron. Then, every matcher compares the submitted trait with the template of the claimed identification, and presents a actual-valued matching rating: the better the score, the higher the similarity. We denote the score of the fingerprint and the face matcher respectively as x_{fing} and x_{face}. Finally, the matching rankings are blended through a right fusion rule to determine whether or not the claimed identity is the person's identification (real consumer) or no longer (impostor).

4.3 Community Intrusion Detection

Intrusion detection systems examine network site visitors to prevent and come across malicious activities like intrusion tries, port scans, and denial-of-service attacks. Eleven while suspected malicious visitors is detected, an alarm is raised via the IDS and eventually handled by using the device administrator. Two main sorts of IDSs exist: misuse detectors and anomaly - based ones. Misuse detectors healthy the analyzed network site visitors against a database of signatures of recognized malicious sports (e.g., snort).The main drawback is that they may beno longer capable of stumble on by no means-before-seen malicious sports, or even editions of recognized ones. Their schooling set is constructed, and periodically up to date to observe the adjustments of regular visitors, through collecting unsupervised community site visitors at some stage in operation, assuming that it's far every-day (it can be filtered via a misuse detector, and ought to be discarded if a few machine malfunctioning happens all through its collection). This type of IDS is susceptible to causative assaults, on the grounds that an attacker might also inject cautiously designed malicious visitors for the duration of the gathering of training samples to pressure the IDS to research a wrong model of the normal traffic. Here we anticipate that an anomaly-primarily based IDS is being designed, the usage of a one-elegance n-SVM classifier with a radial basis function (RBF) kernel and the characteristic vector representation is proposed. Every community packet is taken into consideration as a man or woman sample to be labeled as ordinary (valid) or anomalous (malicious), and is represented as a 256-dimensional characteristic vector, defined because the histogram of byte frequencies in its payload (this is called "1-gram" illustration in the IDS literature). We, then have consciousness on the version choice stage. Within the above setting, it quantities to choosing the values of the n parameter of the gaining knowledge of algorithm (that is an higher sure on the fake effective error charge on education statistics), and the g fee of the RBF kernel. For the sake of simplicity, we anticipate that n is ready to zero:01 as advised, so that simplest g has to be selected.

5. AT EASE DESIGN CYCLE, NEXT STEPS

The classical layout cycle of a pattern classifier consists of: information series, records pre-processing, feature extraction and selection, model choice (along with the choice of the getting to know and category algorithms, and the tuning of their parameters), and overall performance assessment. We pointed out that this layout cycle disregards the threats that could arise in opposed settings, and prolonged the overall performance evaluation step to such settings. Revising the ultimate steps under a safety perspective remains a completely interesting difficulty for destiny work. here we briefly define how this open issue may be addressed. If the adversary is assumed to have some manipulate over the data accrued for classifier training and parameter tuning, a filtering step to detect and put off attack samples have to also be achieved (see, e.g., the data sanitization technique).

Characteristic extraction algorithms have to be designed to be robust to pattern manipulation. as a substitute, features which can be greater hard to be manipulated ought to be used. for example, inexact string matching become proposed to counteract word obfuscation assaults in junk mail filtering. In biometric recognition, it is very common to use additional input functions to detect the presence ("live-ness detection") of attack samples coming from spoofing assaults,

i.e., fake biometric tendencies. The adversary could also undermine characteristic choice, e.g., to pressure the selection of a set of capabilities which might be less complicated to govern, or that are not discriminant sufficient with recognize to future assaults. Therefore, function choice algorithms should be designed by taking into account now not handiest the discriminant functionality, however also the robustness of functions to antagonistic manipulation. Model selection is sincerely the layout step that is greater concern to assaults. selected algorithms must be strong to causative and exploratory assaults. Particularly, robust learning algorithms need to be followed, if no information sanitization may be achieved. using sturdy facts has already been proposed to this intention; especially, to plot studying algorithms robust to a confined amount of information contamination, and class algorithms sturdy to particular exploratory attacks. Eventually, at ease gadget should also guarantee the privacy of its customers, against assaults aimed at stealing personal statistics. As an instance, private-ness keeping strategies have been proposed in biometric popularity structures to defend the customers against the so-referred to as hill-mountain climbing attacks, whose goal is to get records approximately the customers' biometric trends. Randomization of some classifiers parameters has been additionally proposed to maintain privacy.

6 CONTRIBUTIONS, LIMITATIONS AND OPEN PROBLEMS

In this project, we focused on empirical security assessment of sample classifiers that ought to be deployed in adverse environments, and proposed the way to revise the classical performance evaluation layout step, which is not appropriate for this cause. Our most important contribution is a framework for empirical safety assessment that formalizes and generalizes thoughts from preceding work, and may be carried out to exclusive classifiers, gaining knowledge of algorithms, and type obligations. it's miles grounded on a proper model of the adversary, and on a model of facts distribution which can constitute all of the assaults considered in preceding paintings; provides a systematic method for the generation of education and trying out sets that allows security evaluation; and can accommodate application-unique strategies for attack simulation. for example, simulated attack samples can be blanketed into the schooling information to enhance safety of discriminative classifiers (e.g., SVMs), whilst the proposed information version can be exploited to design more at ease generative classifiers. We obtained encouraging initial effects.

REFERENCES

[1] R.N. Rodrigues, L.L. Ling, and V. Govindaraju, "Robustness of Multimodal Biometric Fusion Methods against Spoof Attacks," J. Visual Languages and Computing, vol. 20, no. 3, pp. 169-179, 2009.

[2] P. Johnson, B. Tan, and S. Schuckers, "Multimodal Fusion Vulnerability to Non-Zero Effort (Spoof) Imposters," Proc. IEEE Int'l Workshop Information Forensics and Security, pp. 1-5, 2010.

[3] P. Fogla, M. Sharif, R. Perdisci, O. Kolesnikov, and W. Lee, "Polymorphic Blending Attacks," Proc. 15th Conf. USENIX Security Symp., 2006.

[4] G.L. Wittel and S.F. Wu, "On Attacking Statistical Spam Filters," Proc. First Conf. Email and Anti-Spam, 2004.

[5] D. Lowd and C. Meek, "Good Word Attacks on Statistical Spam Filters," Proc. Second Conf. Email and Anti-Spam, 2005.

[6] A. Kolcz and C.H. Teo, "Feature Weighting for Improved Classifier Robustness," Proc. Sixth Conf. Email and Anti-Spam, 2009.

[7] D.B. Skillicorn, "Adversarial Knowledge Discovery," IEEE Intelligent Systems, vol. 24, no. 6, Nov./Dec. 2009.

[8] D. Fetterly, "Adversarial Information Retrieval: The Manipulation of Web Content," ACM Computing Rev., 2007.

[9] R.O. Duda, P.E. Hart, and D.G. Stork, Pattern Classification. Wiley-Interscience Publication, 2000.

Mr. P.MAHIPAL REDDY was born in India in the year of 1985. He received B.S.C degree in the year of 2006 & M.Tech PG in the year of 2009 from J.N.T.U. He was expert in DataMining, Database Management Systems, Operating system and Computer Network Subjects. He is currently working as An Associate Professor in the CSE Department in Vaagdevi College Of Engineering and Telengana State, India.

Mail ID: mahipalreddy.pulyala@gmail.com

Ms G. Manaimithra was born in India . She is pursuing M.Tech degree in Computer Science & Engineering in CSE Department in Vaagdevi engineering college Bollikunta Warangal and Telengana State, India.

Mail id: manimithrasgs@gmail.com