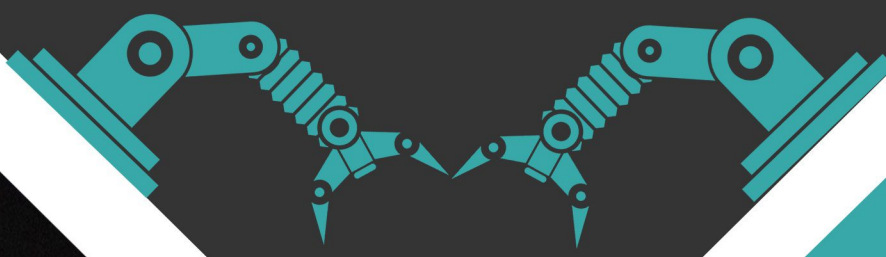
TECH -TALK

THE BIANNUAL MAGAZINE OF COMPUTER SCIENCE AND ENGINEERING



2015-16 ISSUE - II

Computer Science & Engineering Department

VISION

"The Computer Science & Engineering aims at providing continuously stimulating educational environment to its students for attaining their professional goals and meet the global challenges."

MISSION

- To develop a strong theoretical and practical background across the computer science discipline with an emphasis on problem solving.
- To inculcate professional behavior with strong ethical values, leadership qualities, innovative thinking and analytical abilities into the student.
- Expose the students to cutting edge technologies which enhance their employability and knowledge.
- Facilitate the faculty to keep track of latest developments in their research areas. Encourage the faculty to foster the healthy interaction with the industry.

UG – B.TECH
PROGRAMME EDUCATIONAL OBJECTIVES (PEOs)

PEO I: To inculcate the adaptability skills into the students for software design, software development or any other allied fields of computing.
PEO II: To equip the graduates with the ability to analyze, design and synthesize data to create novel products.
PEO III: Ability to understand and analyze engineering issues in a broader perspective with ethical responsibility towards sustainable development.
PEO IV: To empower the student with the qualities of effective communication, team work, continues learning attitude, leadership needed for a successful computer professional.

PROGRAMME OUTCOMES (Pos)

Engineering Graduates will be able to:-

Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

Problem analysis: Identify, formulate, review research literature, and analyze complexen gineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

Design/development of solutions: Design solutions for complex engineering problems anddesign system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

Modern tool usage: Create, select, and apply appropriate techniques, resources, and modernen gineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

The engineer and society: Apply reasoning informed by the contextual knowledge to assesssocietal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

Environment and sustainability: Understand the impact of the professional engineering solutionsin societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms ofthe engineering practice.

Individual and team work: Function effectively as an individual, and as a member or leader indiverse teams, and in multidisciplinary settings.

Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

Project management and finance: Demonstrate knowledge and understanding of theengineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES(PSOs):-

1. Programming Paradigms:

To inculcate algorithmic thinking, formulation techniques and visualization, leading to problem solving skills using different programming paradigms.

2. Data Engineering:

To inculcate an ability to Analyse, Design and implement data driven applications into the students.

3. Software Engineering:

Develop an ability to implement various processes / methodologies /practices employed in design, validation, testing and maintenance of software products.

PG - (M.TECH)

PROGRAMME EDUCATIONAL OBJECTIVES (PEOs)

1. To inculcate the investigating and adaptability skills into the students to carryout research on recent trends in Computer Science and Engineering Technology .
2. To empower the student with the qualities of effective communication, technical document writing, team work, lifelong learning attitude,and leadership needed for a successful career.
3. Enlighten the students on analysing engineering issues in a broader perspective with ethical responsibility towards sustainable development to satisfy the societal needs.
4. Equip the students with all-round knowledge to adapt the evolving technical challenges and changing career opportunities in par with global competency.

Program Outcomes PG Graduates will be able to :-

PO1: Independently carry out research /investigation and development work to solve practical problems

PO2: Write and present a substantial technical report/document

PO3:Demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

PO4: Design and develop software projects given their specifications and within performance and cost constraints.

PO5: An ability to Work on multi-disciplinary projectsand exhibit team skills to upgrade knowledge for adoption of current technological changes.

PO6: Understand the impact of the professional engineering solutionsin societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

Mr. A. S. Rama Chandra Murthy

Asst. Professor

"Sanitizing Private Information Inference Attacks On Social Networks"

Abstract:

Releasing social network data could seriously breach user privacy. User profile and friendship relations are inherently private. Unfortunately, sensitive information may be predicted out of released data through data mining techniques. Therefore, sanitizing network data prior to release is necessary. In this paper, we explore how to launch an inference attack exploiting social networks with a mixture of non-sensitive attributes and social relationships. We map this issue to a collective classification problem and propose a collective inference model. In our model, an attacker utilizes user profile and social relationships in a collective manner to predict sensitive information of related victims in a released social network dataset.

A social network is a graph G(V,E,X) consisting of user set V, friendship link set E and the set of user attribute sets denoted by X. For any user ui,uj∈V (1≤i,j≤|V|), their friendship link ei,j∈E also indicates ej,i∈E.

For an arbitrary user ui, its attribute set is denoted by Xi→∈X (1≤i≤|V|). Each attribute xj∈Xi→ (1≤j≤|Xi→|) is for a certain attribute category hr∈H(1≤r≤|H|), where H is the set of all the categories for a social network. We denote an attribute xj as xj={hr:l1;…;lt}, which means xj is for category hr with value list l1;…;lt where t≥1.

We use Hs⊆H to denote the set of the sensitive categories for a particular user. Any xj∈Xi→ is a sensitive attribute of user ui if xj is for hr∈Hs. Following is an example

H ={Favorite movies, Favorite books, Religion view, Political view}

V ={u1=Jack,u2=Emily}

X1→={x1={Favorite movies: Titanic},x2={Favorite books: Automata; Machine learning}}

X2→={x1={Favorite movies: Pianist},x2={Political view: Conservative}}e1,2∈E,e2,1∈E.

TABLE 1 An Example Information System for a Facebook Data Set

V	h_1: Favorite musical	h_2: Favorite movies	h_3: Favorite books	d: Political view
u_1	Taylor Swift	God's Not Dead	Heaven Is For Real	Conservative
u_2	Carrie Underwood	Son of God	I Declare	Conservative
u_3	Carrie Underwood	God's Not Dead	Heaven Is For Real	Liberal
u_4	George Strait	The Fast and the Furious	Heaven Is For Real	Green
u_5	George Strait	Son of God	I Declare	Liberal
u_6	Taylor Swift	Transformers	The Hunger Games	Conservative
u_7	George Strait	Son of God	The Hunger Games	Liberal
u_8	Taylor Swift	Transformers	I Declare	Conservative

. As shown in Table 1, $V = \{u_1, u_2, \ldots u_8\}$, $C = \{h_1, h_2, h_3\}$, and $D = \{d\}$. Attribute "Favorite movies" of u_1 is assigned value "God's Not Dead".

Generating Decision Rules Based on an Attribute Set

Dataset	No. of UDAs	No. of PDAs - Core	No. of Core
SNAP	7	6	6
Catech	3	2	1
MIT	3	2	1

We address two issues in this paper: (a) how exactly third party users launch an inference attack to predict sensitive information of users, and (b) are there effective strategies to protect against such an attack to achieve a desired privacy-utility tradeoff. For the first issue.

Conclusion:

We show that collectively utilizing both attribute and link information can significantly increase prediction accuracy for sensitive information. For the second issue, we explore the dependence relationships for utility/public attributes, and privacy/public attributes. Based on these results, we propose a Collective Method that take advantages of various data manipulating methods to guarantee sanitizing user data does not incur a bad impact on data utility. Using Collective Method, we are able to effectively sanitize social network data prior to release. The solutions for the two addressed issues are proven to be effective towards three real social datasets.

Ms. M. Sri Bala

Asst. Professor

"Cloud segregating for shared clouds using freight stabilization model for performance enhancement"

Abstract

Cloud computing having tremendous growth on recent years but it is not segregation on shared clouds. Clouds are most provably used for huge amount of data storage and communication. "The cloud", also focuses on increasing the effectiveness of the public resources. Cloud resources are usually not only shared by multiple users but are also vigorously reallocated per demand. This can work for apportioning resources to users .But In the time of apportionment these are indeed .So In this paper we are introducing novel mechanism it represents the Freight stabilization in the cloud computing surroundings has an imperative impact on the performance. Excellent freight stabilizing makes cloud computing more efficient and improves user satisfaction. In this paper we are presenting freight stabilizing techniques for cloud segregating.

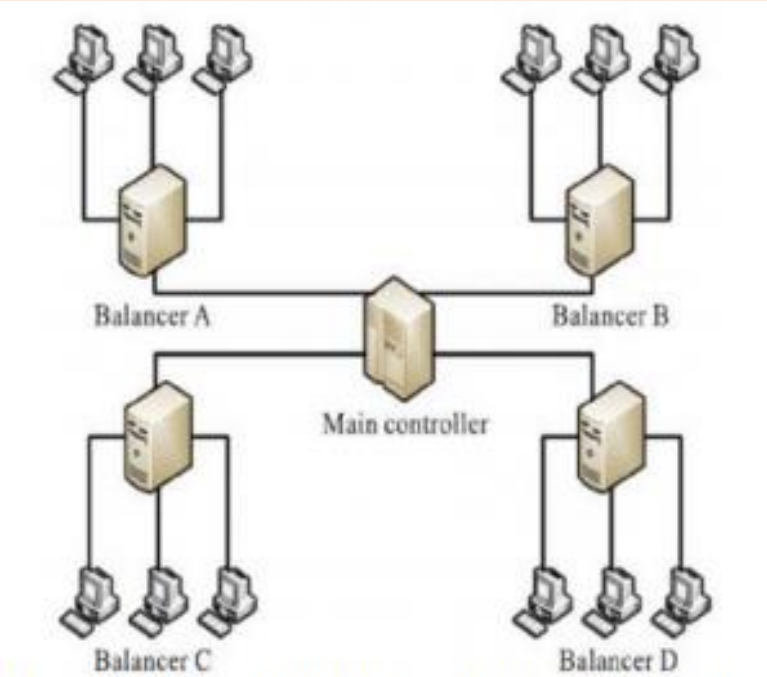


Figure 1: Relationships between the main controllers, the balancers, and the nodes.

Algorithm1: Weighted least connection scheduling algorithm:

Suppose that there is a server set $S=\{S_0,S_1,.....S_{t-1}\}$
Suppose that there is a nodes set in S_i $=\{N_0,N_1,.....N_{m-1}\}$
$W(S_i)$ is the weight of server S_i ;
$W(N_i)$ is the weight of node N_i ;
$C(N_i)$ is the current connection number of server S_i ;
for (k=0; k ≤ m; k++)

```
{
    if(W(Nk)>0)
     {
        for( i=k+1;  i<m; i++)
          {
       If( C(Nk)*W(Ni) > C(Ni)*W(Nk))
              K=i;
          }
       return Nk;
       }
}
return Null;
```

Calculate $CSUM(S_i)=\sum(C(N_i)*W(N_i))$ For $(i = 0,1,2.....m-1)$;
Declare load_factor;
If$(CSUM(S_i) =0;)$
load_factor = idle;
else if $(0 < CSUM(S_i) < W(S_i))$
load_factor = normal;
else if$(CSUM(S_i) \geq W(S_i))$
load_factor = overloaded;

Conclusion

The overall goal of this project is to balance the load on clouds. Stabilizing load on the cloud will improve the performance of cloud services substantially. It will prevent overloading of servers, which would otherwise degrade the performance. The response time will also improve. This software maybe used for efficient data storage on clouds and load stabilizing. This software will help dynamically allocate jobs (data) to the least loaded server.

Thus overall performance of cloud services will not be affected. It aims at having a backup plan in case the system fails even partially. Also work is done to maintain the system stability. There are provisions to accommodate future modifications in the system. Thus, we have successfully gathered information of project and hopefully implement Load Balancing Model for better utilization and performance of cloud services.

Mr. A. Raja Gopal

Asst. Professor

"Object Removal and Image Reconstruction Using Hierarchical Super Resolution Based In painting"

Abstract

This paper introduces novel frame work for Object Removal by means of inpainting. In this method, first the object in the required target area is removed by inpainting. The output thus obtained is given as input to a super-resolution algorithm to recover details on missing areas. Exemplar-based inpainting is used to remove objects that are not required. It is desirable to use a Super-resolution algorithm since inpainting produces a low resolution (LR) image. In this paper a regularization method based on morphologic operations is used for SR image reconstruction. It is always desirable to generate a high resolution (HR) image as it shows more intricate details.

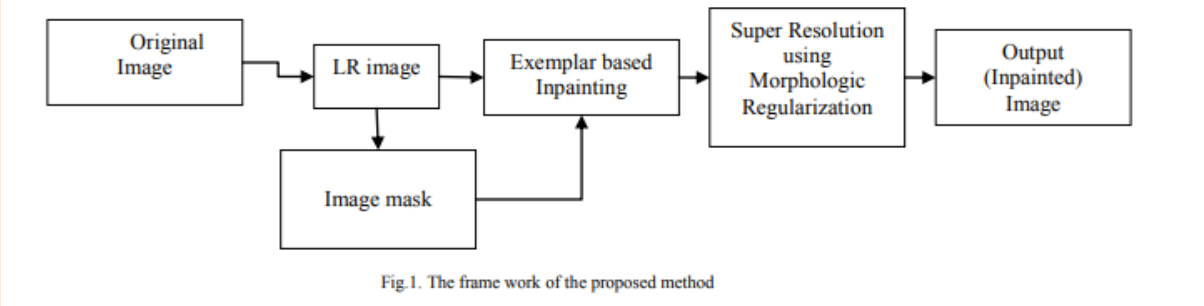


Fig.1. The frame work of the proposed method

ALGORITHM OVERVIEW

This process of inpainting is mainly divided into two sequential steps. The first one is a patch sampling method known as Exemplar based inpainting. The inpainting is performed on a LR (resized) version of an input image. This is because a low resolution picture is less contaminated by noise and is composed of main scene structures. Also, as the picture to inpaint is smaller than the original one, the computation time is reduced compared to the one necessary to inpaint the original image. The inpainted version of the image obtained is given as input to the Super Resolution algorithm. Its goal is to enhance the resolution of the image. shows the frame work of the proposed method which is as follows:

1) A low resolution picture is built from original image

2) An exemplar based inpainting algorithm is applied to remove the object.

3) Super Resolution algorithm is applied to the input image.

Filling order computation:

In order to find the filling order we need to calculate the priority of patches in the filling region. The priority of a patch centered on p is calculated using confidence and data terms. The priority is given by the product of these two terms.

P(p) = C(p) D(p).

Where C(p) is the confidence term and D(p) is the data

$$C(\mathrm{p}) = \frac{\sum_{q \in \psi_p \cap (\mathrm{I} - \Omega)} C(\mathrm{q})}{|\psi_p|}, D(\mathrm{p}) = \frac{\left|\nabla I_p^{\perp} . n_p\right|}{\alpha} \quad (2)$$

Regularization for the SR Reconstruction Algorithm Regularization and iterative methods are used in conjunction for the restoration of noisy degraded images in order to solve an ill posed problem said above. To obtain a stable solution for above equation, we impose a regularization operator ¡ ( ) X on the estimated HR image X. Therefore, the SR image reconstruction problem can simply be formulated as

$$\hat{X} = \arg\min_{X} \{¡\ (X) : \| RHX - Y \|_2^2 < \eta\}$$

The number of unknown pixels in HR grid in X is very large. Therefore a solution to obtain X by inversion may not be feasible. Therefore, an estimate of HR image ˆX is found i.e.,

$$\hat{X} = \arg\min_{X} \left[\| RHX - Y \|_2^2 \right]$$

where η is a scalar constant depending on the noise variance in the LR images. The above equation (10) represents a constrained minimization problem. Unconstrained minimization problem is represented as follows:

$$\hat{X} = \arg\min_{X} \left\{ \frac{1}{2} \| RHX - Y \|_2^2 + \mu \Upsilon(X) \right\}$$

RESULTS

The proposed method is applied on different images and compared with the Patch Match method which is available in Adobe PhotoshopFig. 2 shows the results obtained after applying super resolution based inpainting on different natural images. Column (a) gives the original images, column (b) gives the image masks (object to be removed) and column (c) gives the SR Inpainted images.

Mr. B. Sivarama Krishna

Asst. Professor

"A Computational Trust Model for Peer to Peer Systems to organize itself"

Abstract:

This paper presents distributed algorithms used by a peer to reason about trustworthiness of other peers based on the available local information which includes past interactions and recommendations received from others. Peers collaborate to establish trust among each other without using a priori information or a trusted third party. A peer's trustworthiness in providing services, e.g., uploading files, and giving recommendations is evaluated in service and recommendation contexts. Three main trust metrics, reputation, service trust, and recommendation trust, are defined to precisely measure trustworthiness in these contexts. An interaction is evaluated based on three parameters: satisfaction, weight, and fading effect. When evaluating a recommendation, including to these parameters, recommender's trustworthiness and confidence about the information provided are considered.

Nine different behavior models representing individual, collaborative, and identity changing malicious peers are studied in the experiments. Observations demonstrate that malicious peers are identified by good peers. The attacks are mitigated even if they gain high reputation. Collaborative recommendation-based attacks might be successful when malicious peers make discrimination among good peers. Identity changing is not a good attack strategy.

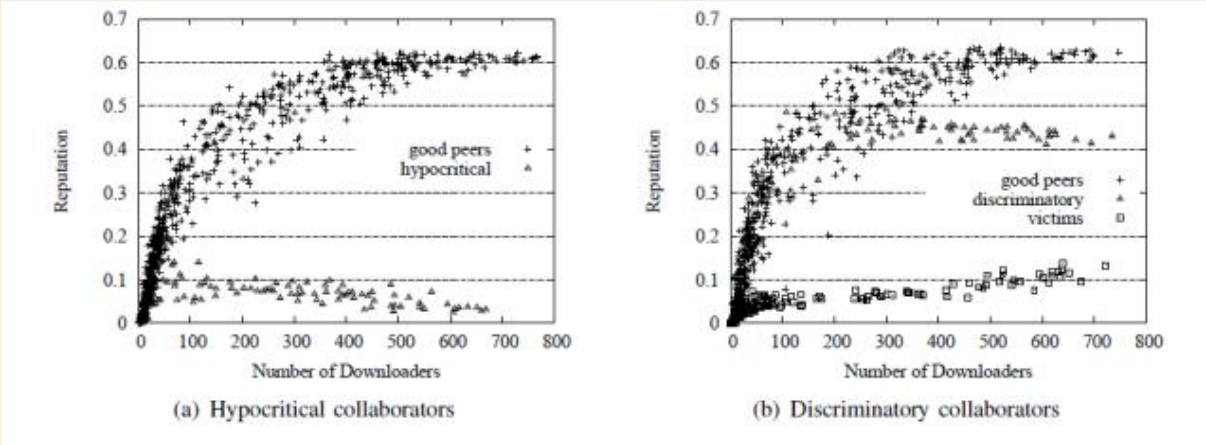
Service Trust Metric (stij)

This section describes the calculation of service trust metric. A peer first calculates competence and integrity belief values using the information about service interactions. Competence belief is based on how well an acquaintance satisfied the needs of interactions . cbij denotes the competence belief of pi about pj in the service context. Average behavior in the past interactions can be a measure of competence belief. pi calculates cbij as follows:

$$cb_{ij} = \frac{1}{\beta_{cb}} \sum_{k=1}^{sh_{ij}} (e_{ij}^{k} \cdot w_{ij}^{k} \cdot f_{ij}^{k})$$

Method

A simulation program has been implemented in Java programming language. Simulation parameters are generated based on the findings of several empirical studies vso observations about the proposed algorithms can be more realistic. Some details of the method will be explained in the next section since they are closely related with the input parameters. Downloading a file is a service interaction. A peer sharing files is called an uploader. A file search request returns all online uploaders in the network. A peer downloads a file from one uploader to simplify integrity checking.



CONCLUSION

A self-organizing trust model for P2P networks is presented in which a peer can develop trust relations without using a priori information. Trust metrics defined on service and recommendation trust contexts help a peer to reason more precisely about capabilities of other peers in providing services and giving recommendations. If all peers are behave good, reputation of a peer is proportional to its capabilities such as network bandwidth, average online period and number of shared files. In a malicious network, service and recommendation-based attacks affect the reputation of a peer. Three individual attacker, three collaborator and three pseudo spoofer behaviors are studied. SORT mitigates service-based attacks in all scenarios.

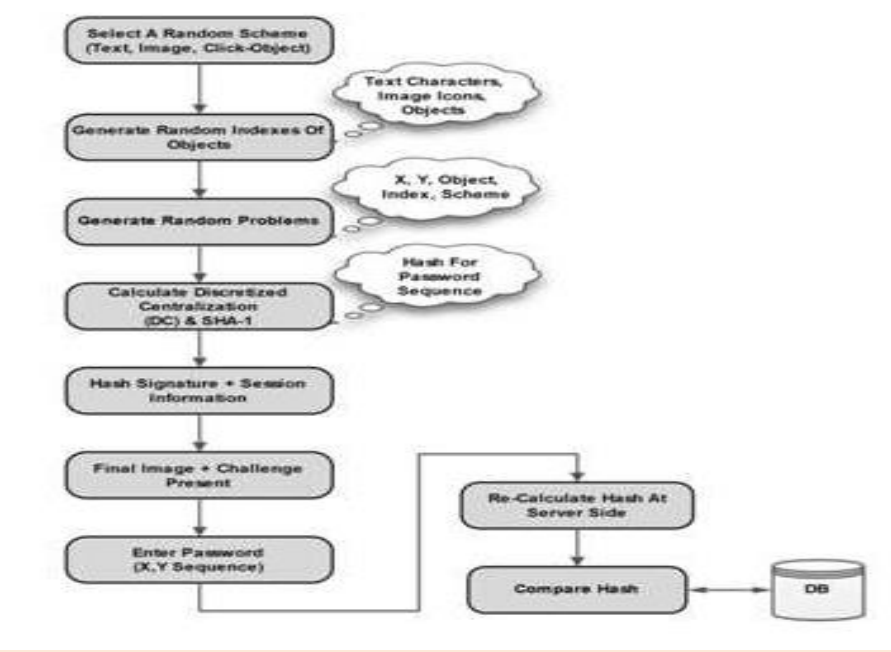
Mr. A. Raja Gopal

Asst. Professor

"Novel Technique for graphical passwords using Captcha"

Abstract

Cyber security is an important issue to tackle. Various user authentication methods are used for this purpose. It helps to avoid misuse or illegal use of highly sensitive data. Text and graphical passwords are mainly used for authentication purpose. But due to various flaws, they are not reliable for data security. Text passwords are insecure for reasons and graphical are more secured in comparison but are vulnerable to shoulder surfing attacks. Hence by using graphical password system and CAPTCHA technology a new security primitive is proposed. We call it as CAPTCHA as gRaphical Password (CaRP). CaRP is a combination of both a CAPTCHA and a graphical password scheme. In this paper we conduct a comprehensive survey of existing CaRP techniques namely ClickText, ClickAnimal and AnimalGrid. We discuss the strengths and limitations of each method and point out research direction in this area. We also try to answer "Are CaRP as secured as graphical passwords and text based passwords?" and "Is CARP protective to relay attack?"



Flowchart of Basic CaRP Authentication of the Proposed Architecture

Step 1: Enter ID and send it to Authentication server AS.

Step 2: AS Stores a salt and hash value H(p, s) for each ID .p is the user password and it is stored.

Step 3: Upon receving login request, AS generates a CARP image. It records location of charcters or animals in image and the image is sent to the user.

Step 4: User Clicks the Password.

Step 5: Co-ordinates of points are recorded are sent to AS.

Step 6: AS maps these Co-ordinates & recovers clickable points of object p, that user clicked.

Step 7: Then AS retrieves salt s of account &calculate its hash value with salt using alsorithm like SHA-1.

Step 8: IT compares result with hash value stored for the a/c.

GRAPHICAL PASSWORD

Graphical password schemes have been proposed as a possible alternative to alphanumeric schemes, motivated partially by the fact that humans can remember images easily than text; psychological studies supports such assumption. Images are generally easier to be remembered than text. In addition, if the number of possible images is enough large, the possible password space of a graphical password scheme may exceed that of text-based schemes and thus presumably offer better resistance to dictionary attacks. Because of these (presumed) advantages, there is a increasing interest in graphical password. Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning.

Conclusion

CaRP schemes are classified as Recognition-Based CaRP and Recognition-Recall CaRP. We have discussed Recognition- Based CaRP which include ClickText, ClickAnimal and AnimalGrid techniques in this paper. Current graphical password techniques are an alternative to text password but are still not fully secure. As a framework, CaRP does not rely on any specific CAPTCHA scheme. When one CAPTCHA scheme is broken, a new and more secure one may appear and be converted to a CaRP scheme.

Mr. J. Nageswara Rao

Assistant Professor

"Effective Video Sharing In Online Social Network"

ABSTRACT

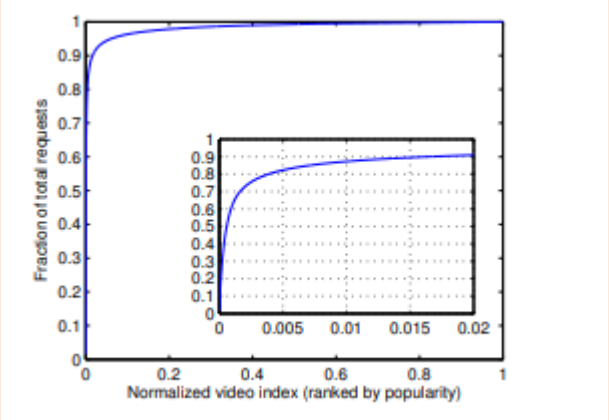
Online social networks (OSNs) have become popular destinations for connecting friends and sharing information. Recent statistics suggest that OSN users regularly share contents from video sites, and a significant amount of requests of the video sites are indeed from them nowadays. These behaviors have substantially changed the workload of online video services. Moreover, we observe that the requests for the new published videos generally experience two or three days latency to reach the peak value, and then change dynamically with a series of unpredictable bursts (while in YouTube, videos reach the global peak immediately after introduction to the system, and then the accesses generally decrease overtime, except possibly on some special days). These differences can raise new challenges to content providers.
VIDEO POPULARITY DISTRIBUTION

Table 1: Summary of trace in one-day period

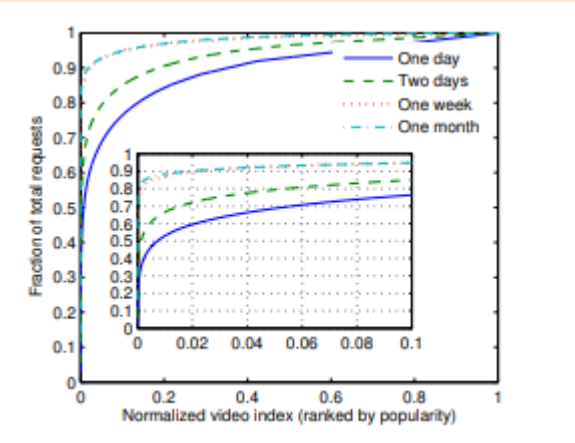
Views	Shares	Users	Videos	NewVideos
12,432,708	1,628,852	3,514,461	201,517	71,236

Pareto Principle

The Pareto principle (also known as the 80-20 rule) is widely used to describe the skewness in distributions. For example, the analysis of YouTube shows that 10% of the most popular videos account for 80% of user request. It is interesting to see whether the social-network-based sharing amplifies or smooths this skewness. As shown in Fig, we can see a dramatically skewed result that 0.5% videos account for more than 80% of the total requests (the x-axis of this figure represents the videos sorted from the most popular videos to the least popular ones, with video ranks being normalized between 0 and 1); and top-2% videos account for 90% of the total requests.



Skewness of requests across all videos



Requests of videos initially shared on the same day

Our measurement has shown distinctive popularity distribution pattern for video sharing in OSNs. To further testify whether the OSN-based spreading mechanism is the underlying reason for these features, we develop a simple yet effective model to make some preliminary analysis.

Validation and Analysis

We first validate whether our model can reflect the real video spreading process in OSNs by inputting the parameters extracted from RenRen. For the number of videos and requests, we configure the same values (63,591 and 2,905,276) as those in Fig. 3. To get the distribution of BrF in RenRen, we collect all 1628852 shares created on March 24th and count the followed requests separately over three months. The distribution along with the fitting function are shown in Fig. We also notice that the average BrF does not have obvious correlation with the total requests of a video ($\rho p = -0.001$ and $\rho s = -0.15$). We thus configure all videos with the same BrF distribution

Conclusions

Our measurement showed that videos exhibit different popularity distribution pattern compared with that in VSSes. Particularly, it shows much more popularity skewness in the OSN. We further developed a model to simulate the video spreading process in OSNs, and validated that the OSN-based spreading mechanism is the fundamental reason under such new video popularity distribution. We also made some preliminary measurement on the video popularity evolution in OSNs and revealed some distinctive features, such as the randomness, unpredictability, and multiple peaks. To capture such popularity evolution features, some enhancements are needed for our current model, and we will take this for the future work.

Ms. M. Sri Bala

Asst. Professor

"A Novel Technique to Detect the Misbehaviour nodes in Delay Tolerant Networks"

Abstract

Malicious and selfish behaviors represent a serious threat against routing in Delay/Disruption Tolerant Networks (DTNs). Due to the unique network characteristics, designing a misbehavior detection scheme in DTN is regarded as a great challenge. iTrust, a probabilistic misbehavior detection scheme, for secure DTN routing towards efficient trust establishment. The basic idea of iTrust is introducing a periodically available Trusted Authority (TA) to judge the node's behavior based on the collected routing evidences and probabilistically checking. iTrust model as the Inspection Game and use game theoretical analysis to demonstrate that, by setting an appropriate investigation probability, TA could ensure the security of DTN routing at a reduced cost.

Proposed Methodology

In some hybrid DTN network environment, the transmission between TA and each node could be also performed in a direct transmission manner (e.g., WIMAX or cellular networks). Argue that since the misbehavior detection is performed periodically, the message transmission could be performed in a batch model, which could further reduce the transmission overhead. Only consider either of misbehavior detection or incentive scheme Firstly, introduced data forwarding evidences for a general misbehavior detection framework based on a series.

.

Route Discovery and Data Forwarding

A normal user will honestly follow the first routing protocol by forwarding the messages as long as there are enough contacts. The requested message has been forwarded to the next hop, the chosen next hop nodes are desirable nodes according to a specific DTN routing protocol, and the number of forwarding copies satisfy the requirement defined by a multi-copy forwarding routing protocol.

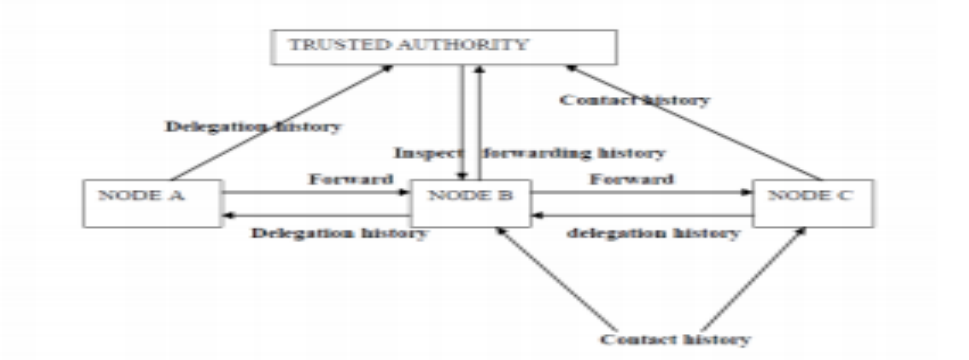


Fig: Syste Architecture

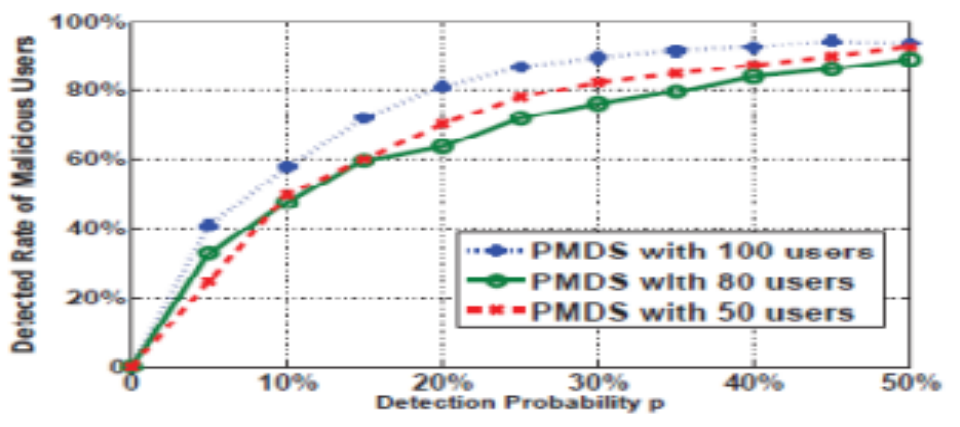


Fig:Detected Rate Of Malicious Node

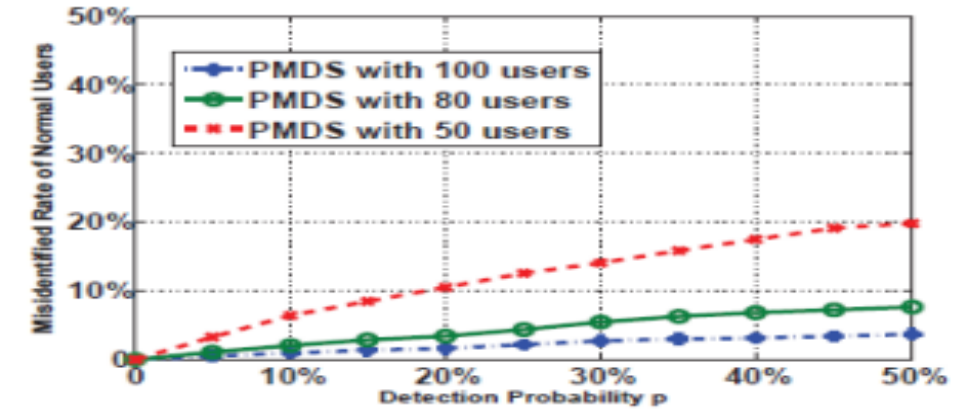


Fig:False Rate Of Misidentified Node

Conclusion

A Probabilistic Misbehaviour Detection Scheme (iTrust), which could reduce the detection overhead effectively.The simulation results confirm that iTrust will reduce transmission overhead incurred by misbehaviour 68 detection and detect the malicious nodes effectively and the future Enhancement will focus on the extension of iTrust to other kinds of networks and reduces the bandwidth of the Trusted Authority by time variant monitoring of the nodes for malicious detection.

Mr. D. Srinivasa Rao

Sr. Asst. Professor

"Analysis of different Utility Mining Methodologies in Transactional databases"

Abstract

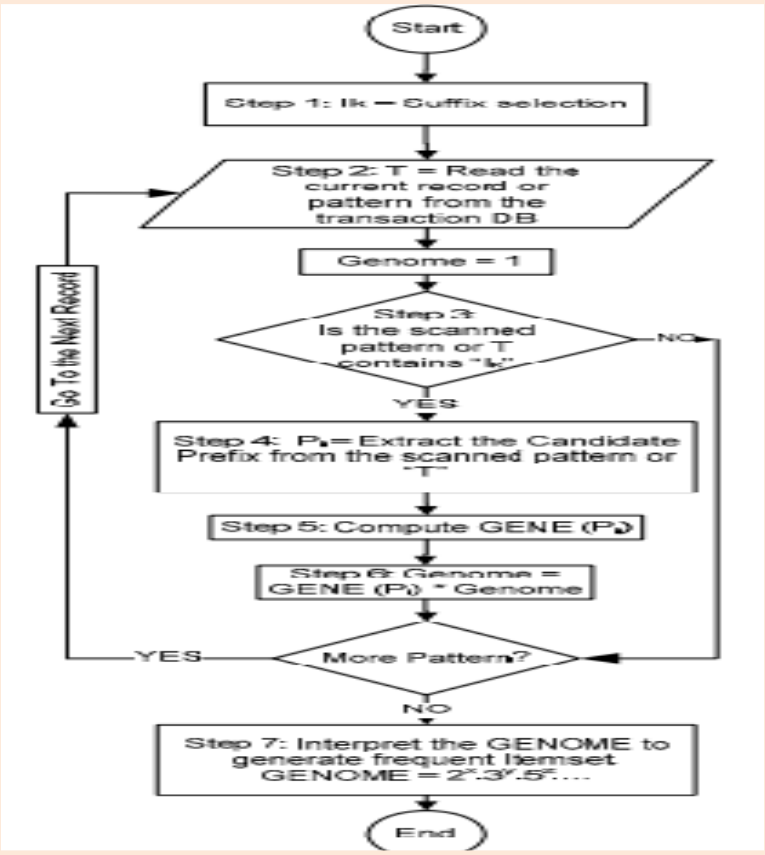
Utility Mining may be delineated as an motion that analyze the data and draws out a few new nontrivial information from the big amount of databases. traditional data mining methods have focused on finding the statistical correlations between the items which are often acting within the database. high software itemset mining is a place of studies where application primarily based mining is a descriptive type of information mining, geared toward locating itemsets that dedicate maximum to the entire software.

FP-Growth Procedurefor Pattern Mining

The essential theorem of mathematics says that every positive integer has a completely unique high factorization. What the FP-growth does is getting a not unusual suffix after which extracts all viable prefixes and after joining them to the suffix a common pattern is created. In the FP-growth set of rules it isn't always crucial that we are searching out all common patterns cease to a selected suffix like "I5" or we want to extract all the frequent patterns. In contrast with FP-increase the FPPF for mining of all frequent styles cease to a specific suffix like "I5", does no longer create complete of the tree and just makes a speciality of prefixes related to that specific suffix.

L = I1: SUP(I1), I2: SUP(I2), …, In: SUP(In) wherein: *ƒ* "Ii" is a frequent itemset with period 1. "SUP (Ii)" is a support count of itemset "Ii" that's extra than minimal support be counted.*ƒ* "L" is looked after descending primarily based on aid depend, because of this SUP (Ii) > SUP (Ii+1). As an example regarding table 1 the L set is I2:7, I1:6, I3:6, I4:2, I5:2.

Definition 2.2: A sample or itemset "T" with period m is represented as T = I1, I2, …, Im such that "Ij" represents the object in "jth" function of "T". for example if T = a, b, c then "I1" is the item "a". all the patterns "Ti" is taken care of in "L" order which means SUP(Ii) > SUP(I(i+1)).



Definition 2.3: Set "M" is described as a set of all styles or itemsets which is also referred to as the transaction desk, and is represented as M = T1,T2,…,Tn in which "T" is a sample or itemset (Definition 2.2).

Conclusion

Most of research on high utility item set focuses on static databases (eg.Transaction database). With the emergence of the new application, the data processed may be in the continuous dynamic data streams. Because the data in streams come with high speed and are continuous and unbounded, mining result should be generated as fast as possible and make only one pass over a data. In this paper, we have proposed two algorithms named UP-Growth and UP-Growth+ forming in high utility item sets from transaction databases. A data structure named UP-Tree was proposed for maintaining the information of high utility item sets.PHUIs can be efficiently generated from UP-Tree with only two databases cans.

NCC

B Enrollments

Sr.No	RGTL NO	NAME OF THE CADET
1	APSW/2015/372552	GAVIRINENI BABY SINDHUJA
2	APSW/2015/372553	KONDURU RUPA MOUNIKA
3	APSW/2015/372554	MEDURI PRABHATHA
4	APSW/2015/372555	VELUGULETI C N D SINDHUSA
5	APSW/2015/372556	GANAGARAJU SUDHA MADHURI
6	APSW/2015/372557	CHILLA BHUVANESHWARI
7	APSW/2015/372558	PARVATANENI GEETHIKA
8	APSW/2015/372559	KAREDLA POOJITHA
9	APSW/2015/372560	BOMMADEVARA MONICA BHAVANI
10	APSW/2015/372561	VENNAPUSA SRAVANTHI
11	APSW/2015/372562	CHALLA JERUSA ESTHER RANI
12	APSW/2015/372563	KIRANMAI MEDISETTI
13	APSW/2015/372564	BI BI AYEESHA
14	APSW/2015/372565	SHAIK RUBEENA
15	APSW/2015/372566	MOHAMMAD KARISHMA
16	APSW/2015/372567	B N S D KAMESWARI
17	APSW/2015/372568	VALLURU PRATHYUSHA

SAHELI Club Events

- An awareness program on "A Community Awakening Caravan To Counter Trafficking" was conducted at LBRCE on 29-02-2016.
- Seminar on "Youth-The Future Of India" organized on 22nd December 2015.

Editorial Board

Dr.N. Ravi Shankar
Professor & HOD
CSE Department

Mr. D. Veeraiah
Associate Professor
CSE Department

Mr. G. Balu Narasimharao
Asst. Professor
CSE Department

Aman
CSE IV

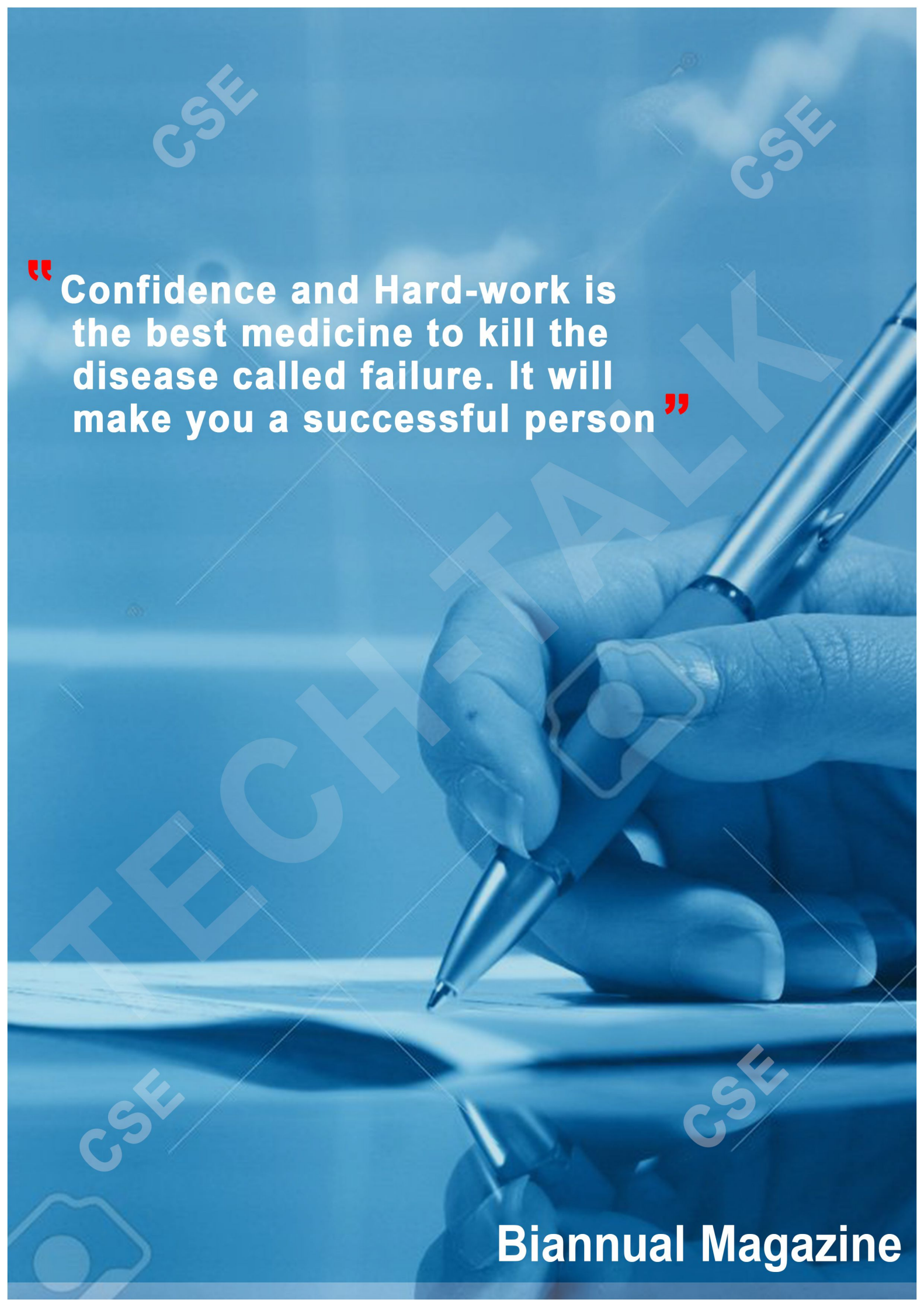
Tireesha
CSE III

Acknowledgements

At the end, we would like to extend our sincere gratitude to our management for their constant support. Also we would like to thank our Director, Dr. E. V. Prasad and Mentor Dean, Dr. R. Chandrashekaram for their encouragement. We would also like to thank our HOD Dr. N. Ravi Shankar for the innovative ideas for the additions made to our magazine, and Faculty for shaping the TECH-TALK. Also our gratitude to our fellow members of the editorial board and department for their support to the TECH-TALK. Lastly we would like to thank all the faculty members, students and all stakeholders for their valuable inputs.

-The Editorial Team
TECH-TALK

LAKIREDDY BALI REDDY COLLEGE OF ENGINEERING
(AUTONOMOUS)
Approved by AICTE, NEW DELHI, Affiliated to JNTUK, Kakinada
Accredited by NAAC (A) UGC, NBA Accredited, ISO 9001:2008
Certified Institution
MYLAVARAM – 521 230, Krishna Dist., A. P. INDIA.
Tel: 08659-222933, 934, 94401 39918 Fax: 08659-222931


"Confidence and Hard-work is the best medicine to kill the disease called failure. It will make you a successful person"
CSE
CSE
CSE
CSE
TECHTALK
Biannual Magazine