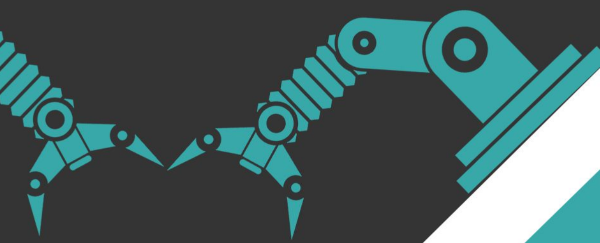
TECH -TALK

THE BIANNUAL MAGAZINE OF COMPUTER SCIENCE AND ENGINEERING



2016-17 ISSUE - I

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.

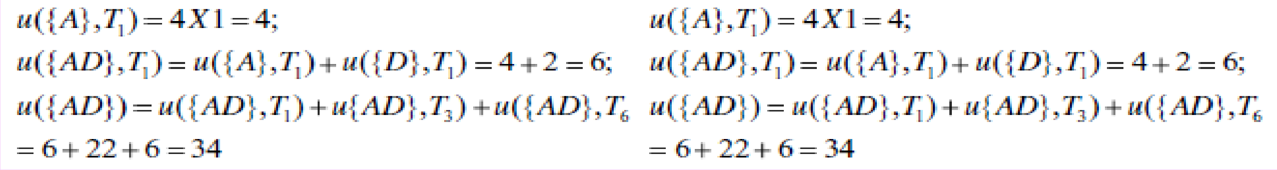
Mr. D. Srinivasa Rao

Sr. Asst. Professor

"Maximum Utility Item sets for Transactional databases using GUIDE"

Abstract

The issue of high utility mining is finding the majority of the high utility item sets in a value-based database. Most calculationsdiscover high utility item sets in two stages. The initial step distinguishes the greater part of the potential item sets. The second step then decides the high utility item sets from the arrangement of potential item sets. The extensive number of potential item sets in the initial step is for the most part the mining bottleneck. In the event that we can diminish the quantity of potential item sets, the mining execution can be enhanced essentially. In this paper we propose a novel structure, named GUIDE (Generation of maximal high Utility Item sets from Data streams), to discover maximal high utility item sets from information streams with distinctive models, i.e., historic point, sliding window and time blurring models. The proposed structure, named MUI-Tree (Maximal high Utility Item set Tree), keeps up vital data for the mining procedures and the proposed techniques further

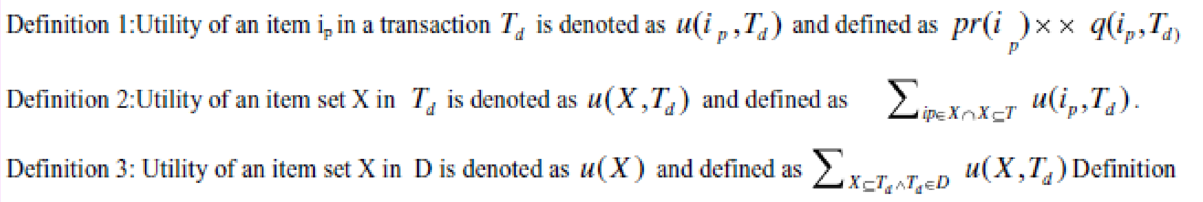


$u(\{A\},T_1) = 4X1 = 4;$ $u(\{A\},T_1) = 4X1 = 4;$

$u(\{AD\},T_1) = u(\{A\},T_1) + u(\{D\},T_1) = 4+2 = 6;$ $u(\{AD\},T_1) = u(\{A\},T_1) + u(\{D\},T_1) = 4+2 = 6;$

$u(\{AD\}) = u(\{AD\},T_1) + u\{AD\},T_3) + u(\{AD\},T_6$ $u(\{AD\}) = u(\{AD\},T_1) + u\{AD\},T_3) + u(\{AD\},T_6$

$= 6+22+6 = 34$ $= 6+22+6 = 34$



Definition 1:Utility of an item i_p in a transaction T_d is denoted as $u(i_p, T_d)$ and defined as $pr(i_p) \times \times \ q(i_p, T_{d)}$

Definition 2:Utility of an item set X in T_d is denoted as $u(X, T_d)$ and defined as $\sum_{ip \in X \cap X \subseteq T} u(i_p, T_d)$.

Definition 3: Utility of an item set X in D is denoted as $u(X)$ and defined as $\sum_{X \subseteq T_d \wedge T_d \in D} u(X, T_d)$ Definition

Time-sensitive window:

The window for a settled timeframe, for example, one month; Transactiondelicate window: The window for altered size of exchanges, for example, ten thousand exchanges. In this paper, we talk about the time-touchy window. Note that the proposed system can fit both sorts of windows. For managing the instance of exchange touchy window, the proposed technique just needs to supplant thetime by the TID for the exchanges.

In this subsection, the execution assessment about the calculations for the sliding window model is displayed. To begin with, we demonstrate the execution correlation under differed least utility edges. The tried dataset is D50kT5N1000. The outcomes are appeared in Figure

1. It can be watched that the execution of GUIDESW is the best, trailed by MHUI-TID, and THUI-Mine be the most exceedingly bad. Moreover, in Figure 1 (an) and (b), GUIDESW performs more awful than GUIDELM on runtime as well as memory utilization. It is on account of that the redesign ever openings ought to be managed in GUIDESW.

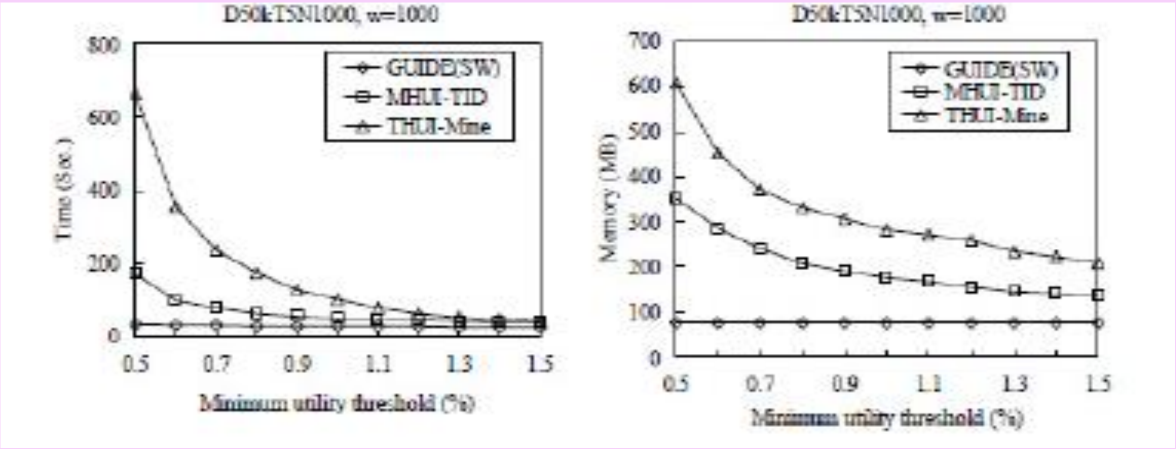


Fig 1. Evaluation of varying minimum utility threshold

In the analyses, we can see that not just the runtime of GUIDELM outflanks that of GUIDESW additionally those of MHUI-TID and THUI-Mine in historic point model beat those in sliding window model. The reason is that in spite of the fact that the strategies for historic point model need to prepare the entire information from the milestone time, those for sliding window model need to perform the tedious procedures for redesigning data when windows slide at every time point.

Conclusion

In this paper, we proposed a novel system, to be specific GUIDE, for effectively mining maximal high utility item sets from information streams. The strategies for distinctive models point of interest, sliding window and time blurring are proposed. The proposed conservative information structure MUI-Trees are collaborated with the techniques for putting away crucial data in information streams. Additionally, two compelling and proficient procedures are proposed for following and pruning the MUI-Trees. Fundamental commitments of this work are recorded as takes after: 1) This work first addresses the issue of finding conservative types of high utility item sets from information streams; 2) GUIDE is a successful one-pass structure which meets the necessities of information stream mining; 3) MUI-Tree keeps up key data for the mining procedures and the proposed methodologies further

Mr. G. Balu Narasimharao

Assistant Professor

"Mitigating the Malicious Nodes by the Effect of Trust Evaluation with Composite Trust Public Key Management in MANET"

Abstract

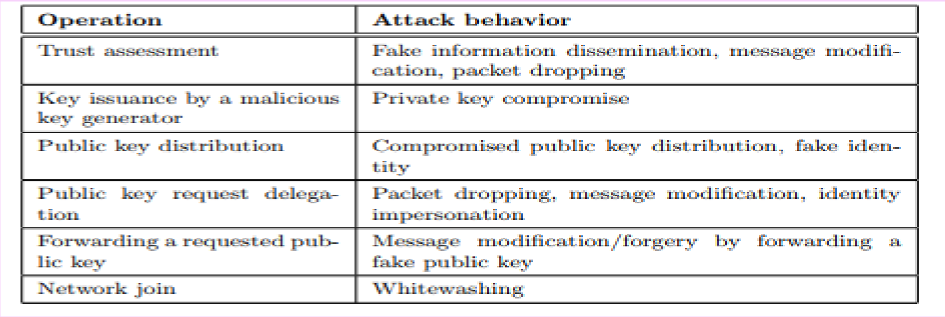
Public key management in mobile ad hoc networks (MANETs) has been studied for several decades. However, the unique characteristics of MANETs have imposed great challenges in designing a fully distributed public key management protocol under resource-constrained MANET environments. These challenges include no centralized trusted entities, resource constraints, and high security vulnerabilities. This work proposes a fully distributed trust-based public key management approach for MANETs using a soft security mechanism based on the concept of trust. Instead of using hard security approaches, as in traditional security techniques, to eliminate security vulnerabilities, our work aims to maximize performance by relaxing security requirements based on the perceived trust. We propose a composite trust-based public key management (CTPKM) with the goal of maximizing performance while mitigating security vulnerability. Each node employs a trust threshold to determine whether or not to trust another node. Our simulation results show that an optimal trust threshold exists to best balance and meet the conflicting goals between performance and security, by exploiting the inherent tradeoff between trust and risk. The results also show that CTPKM minimizes risk (i.e., information leakout) using an optimal trust threshold while maximizing service availability with acceptable communication overhead incurred by trust and key management operations. We demonstrate that CTPKM outperforms both existing non-trust-based and trust-based counterparts.

Hybrid Public Key Management

Some researchers proposed hybrid public key management mechanisms that combine the features of multiple schemes to meet the requirements. Sun et al combined ID-based key management with threshold cryptography without using a centralized third party to deal with key management] combined certificate less public key cryptography which eliminates the key escrow problem with threshold cryptography which does not require a centralized third party. Zhang et al. proposed an ID-based key management scheme that combines ID-based cryptography with threshold cryptography to enhance security and reduce communication cost for key management. Li et al. also proposed a hybrid key management scheme combining ID-based key management and threshold cryptography

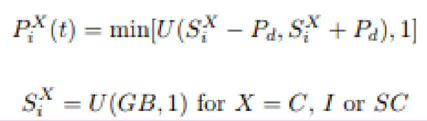
Fake identity / impersonation:

A node may use a fake identity or multiple identities (i.e., Sybil attack) to break information confidentiality in communications between two entities. In particular, a node can impersonate as a victim node whose private key is compromised by distributing the public key and the certificate of the victim node to its neighbors in order to attract the victim node's packets to it. However, when the corresponding private key compromise attack is detected (explained above), the public/private key pairs of the victim node will be denounced. If an attacker continues to use the private/public key pairs to do fake identity attack, it will be detected and the detection will attribute to lowering trust in integrity



Operation	Attack behavior
Trust assessment	Fake information dissemination, message modification, packet dropping
Key issuance by a malicious key generator	Private key compromise
Public key distribution	Compromised public key distribution, fake identity
Public key request delegation	Packet dropping, message modification, identity impersonation
Forwarding a requested public key	Message modification/forgery by forwarding a fake public key
Network join	Whitewashing

Fig : Attack behavior for operations



$$P_i^X(t) = \min[U(S_i^X - P_d, S_i^X + P_d), 1]$$

$$S_i^X = U(GB, 1) \text{ for } X = C, I \text{ or } SC$$

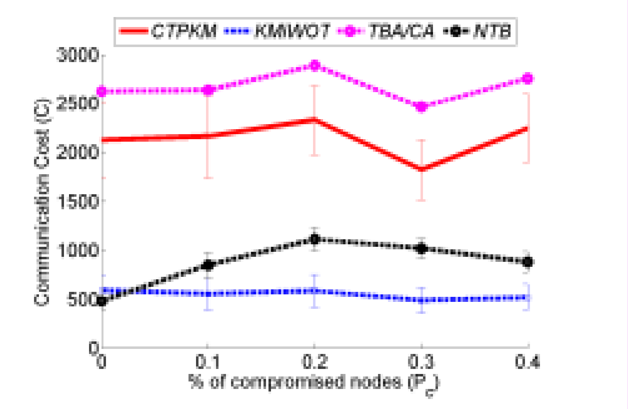


Fig: Effect of percentage of compromised nodes (Pc) on trust bias and performance

Conclusion

In this paper, we proposed a composite trust based public key management scheme (CTPKM) for MANETs. Considering three different trust dimensions, namely, competence, integrity, and social contact, CTPKM enables a node to make decisions while interacting with others based on their trust levels. We devised four performance metrics to analyze the impact of our trust threshold based public key management design on security vulnerability.

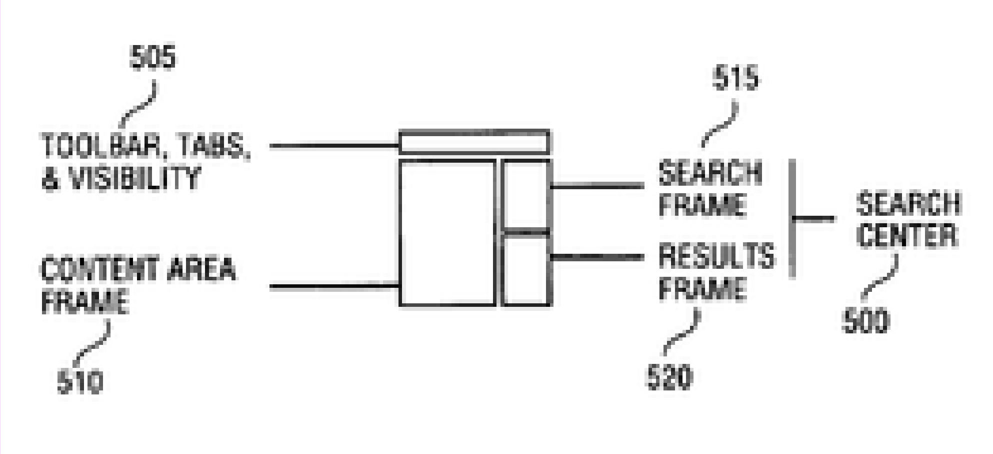
Mr. G Nageswara Rao

Associate Professor

"Integrated framework for multiuser encrypted query operations on cloud data base services"

Abstract

According to one aspect of the present invention, a method includes displaying a search tool bar including a search icon. The method also includes displaying a search center pane after a user selects the search icon, wherein the search center pane includes a search frame. The method further includes selecting a search category from a dropdown list of search categories in the search frame. In addition, the method includes entering a search keyword. Furthermore, the method includes searching a database for data records matching the search category and the search keyword.



The present invention relates generally to the field of data processing. More specifically, the present invention relates to a system and method to implement an integrated search center supporting a full-text search and a query on a database.

As technology continues to advance and the business environments have become increasingly complex and diverse, more and more companies have relied on various customer relationship management (CRM) software and eBusiness applications to conduct and manage various aspects of their enterprise business. In general, eBusiness applications are designed to enable a company or enterprise to conduct its business over an interactive network (e.g., Internet, Intranet, Extranet, etc.) with its customers, partners, suppliers, distributors, employees, etc. eBusiness applications may include core business processes, supply chain, back-office operations, and CRM functions. CRM generally includes various aspects of interaction a company has with its customers, relating to sales and/or services. At a high level, customer relationship management is focused on understanding the customer's needs and leveraging this knowledge to increase sales and improve service. CRM application and software is generally designed to provide effective and efficient interactions between sales and service, and unify a company's activities around the customer in order to increase customer share and customer retention through customer satisfaction.The metrics of success were based on efficient delivery of service and operating the customer call center as inexpensively as possible. Customer interaction was considered a “cost” of doing business.

System Overview and Overall Architecture

In one embodiment, a system in which the teachings of the present invention are implemented can be logically structured as a multi-layered architecture as shown in FIG. 1. In one embodiment, the logical multi-layered architecture as shown in FIG. 1 provides a platform for common services to support the various applications. These services may include a user interface layer 110, an object manager layer 120, a data manager layer 130, and a data exchange layer 14

Generally, eBusiness applications are designed to allow organizations to create a single source of customer information that makes it easier to sell to, market to, and service customers across multiple channels, including the Web, call centers, field, resellers, retail, and dealer networks. Advanced eBusiness applications are typically built on a component-based architecture and are designed to be Web-based and to deliver support for various types of clients on multiple computing platforms including mobile clients, connected clients, thin clients, and handheld clients, etc

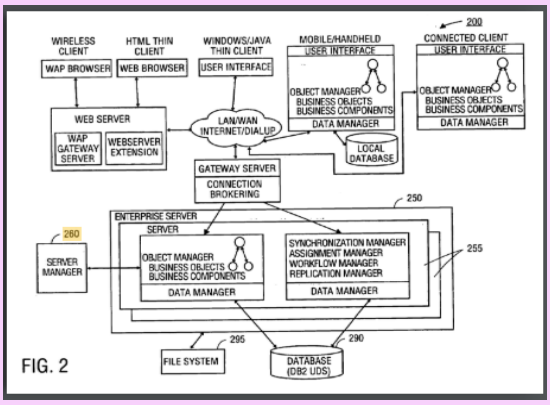


FIG. 2

Conclusion

The method also includes displaying a search center pane after a user selects the search icon, wherein the search center pane includes a search frame. The method further includes selecting a search category from a dropdown list of search categories in the search frame. In addition, the method includes entering a search keyword. Furthermore, the method includes searching a database for data records matching the search category and the search keyword.

Mr. A. Sudhakar

Assistant Professor

"Prediction policy based technique for multimedia content sharing in social network sites"

Abstract

Usage of social media's has been considerably increasing in today's world which enables the user to share their personal information like images with other users. This improved technology leads to privacy violation where the users can share large number of images across the network. To provide security for the information, we put forward this paper consisting Adaptive Privacy Policy Prediction (A3P) framework to help users create security measures for their images. The role of images and its metadata are examined as a measure of user's privacy preferences. The Framework determines the best privacy policy for the uploaded images. It includes an Image classification framework for association of images with similar policies and a policy prediction technique to automatically generate a privacy policy for user-uploaded images.

SYSTEM ARCHITECTURE

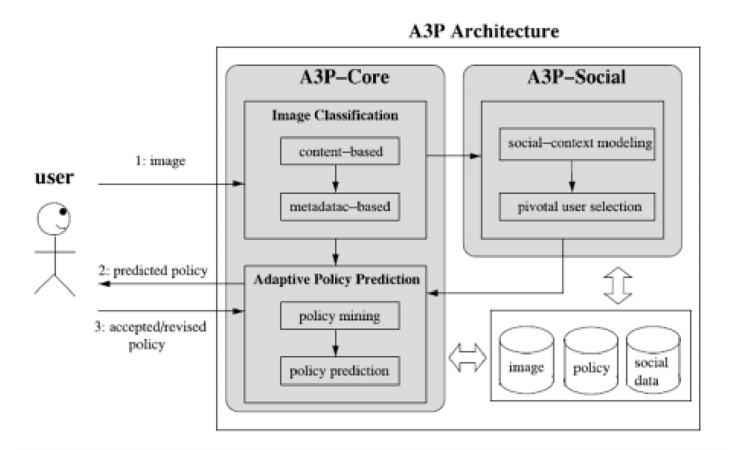


Fig.1 System Overview

A3P stands for Adaptive Privacy Policy Prediction system which helps users to derive the privacy settings for their images.

The A3P Architecture consists of followings blocks: Metadata based Image classification, Adaptive policy prediction ,Look-Up Privacy Policies ,Database.

Adaptive Policy Prediction

The policy prediction algorithm provides a predicted policy of a newly uploaded image to the user for his/her reference. More importantly, the predicted policy will reflect the possible changes of a user‟s privacy concerns. The prediction process consists of three main phases:

Policy normalization: The policy normalization is a simple decomposition process to convert a user policy into a set of atomic rules in which the data (D) component is a single-element set.

Policy mining: Policy mining is carried out within the same category of the new image because images in the same category are more likely under the similar level of privacy protection. The basic idea of the hierarchical mining is to follow a natural order in which a user defines a policy.

Steps of policy mining

Step 1: This process apply association rule mining on the subject components of the policies of the new image. With the association rule mining we select the best rules according to one of the interestingness measure i.e., support and confidence which gives the most popular subjects in policies.

Step 2: This process apply association rule mining on the action components. Similar to the first step we will select the best rules which will give most popular combinations of action in policies.

Step 3: This process mine the condition component in each policy set. The best rules are selected which gives us a set of attributes which often appear in policies.

Policy Prediction: The policy mining phase may give us many policies but our system needs to show the best one to the user. Thus, this approach is used to choose the best policy for the user by obtaining the strictness level. Different integer values are assigned according to the strictness to the combinations and if the data has multiple combinations we will select the lowest one. Hence if he specifies policy as “friends”=male, then the coverage rate can be calculated as (3/5)=0.6. Hence, the image is less restricted if the coverage rate value is high.

CONCLUSION

In this paper we examine the role of social context, image content, and metadata as possible indicators of users‟ privacy preferences with the increasing volume of images users share through social sites, maintaining privacy has become a major problem, as demonstrated by a recent wave of publicized incidents where users inadvertently shared personal information. By using this we can easily prevent unwanted discloser and privacy violations. Unwanted discloser may lead to misuse of one‟s personal information .users automate the privacy policy settings for their uploaded images with the help of adaptive privacy policy prediction (a3p). Based on the information available for a given user the a3p system provides a comprehensive framework to infer privacy preferences. A3p system is a practical tool.

Dr. D. Veeraiah

Associate Professor & Head, Information Center

"An enhanced approach of secure pattern classification under attack"

Abstract

Design order frameworks are usually utilized as a part of ill-disposed applications, as biometric confirmation, system interruption location, and spam separating, in which information can be intentionally controlled by people to undermine their operation. As this ill-disposed situation is not considered by traditional outline strategies, design characterization frameworks may display vulnerabilities, whose misuse may extremely influence their execution, and thus restrain their pragmatic utility. Amplifying design grouping hypothesis and outline strategies to ill-disposed settings is therefore a novel and exceptionally significant exploration bearing, which has not yet been sought after efficiently. In this project, we address one of the fundamental open issues: assessing at configuration stage the security of example classifiers, specifically, the execution debasement under potential assaults they may bring about amid operation. We propose a novel technique for online alert aggregation which is based on a dynamic, probabilistic model of the current attack situation. Basically, it can be regarded as a data stream version of a maximum likelihood approach for the estimation of the model parameters.

In this work we address issues above by building up a structure for the experimental assessment of classifier security at outline stage that develops the model choice and execution assessment ventures of the established configuration cycle . We compress past work, and bring up three fundamental thoughts that rise up out of it. We then formalize and sum them up in our structure. Averts creating novel strategies to survey classifier security against these assault. The nearness of an insightful and versatile foe makes the grouping issue exceedingly non-stationary .

ONLINE ALERT AGGREGATON ALGORITHM

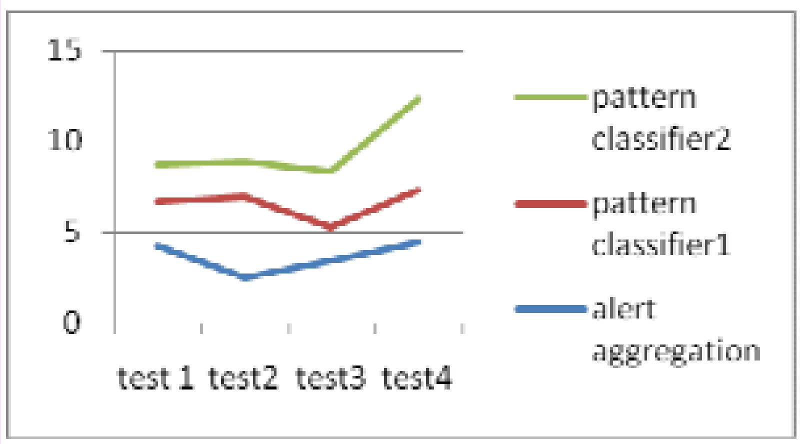
STEP1: If a new alert is observed we first have to decide whether a first component has to be created.
STEP2: initialize its parameters with information taken from this alert. Random, small values are added
STEP3: decide whether the alert has to be associated with an existing component or not
STEP4: it belongs to an ongoing attack instance or not.
STEP5: Sequences of meta-alerts may be investigated further in order to detect more complex attack scenarios.

STEP6: Meta-alerts may be exchanged with other ID agents in order to detect distributed attacks such as one-tomany attacks.

STEP7: Based on the information stored in the meta-alerts, reports may be generated to inform a human security expert about the ongoing attack situation

Attack Simulation:

In this module, the attack simulation is made for ourself to test the system. Attacks are classified and made to simulate here. Whenever an attack is launched the Intrusion Detection System must be capable of detecting it. So our system will also be capable of detecting such attacks. For example if an IP trace attack is launched, the Intrusion Detection



Finally the result indicates the intrusion detection accuracy is improved compared with earlier techniques by running different tests.

CONCLUSION:

The tests showed the wide relevance of the proposed online ready total methodology. We broke down three distinct information sets and demonstrated that machine-learning-based finders, routine signature based finders, and even firewalls can be utilized as ready generators. In all cases, the measure of information could be lessened generously Our fundamental commitment is a system for observational security assessment that formalizes and sums up thoughts from past work, and can be connected to various classifiers, learning calculations, and grouping assignments. It is grounded on a formal model of the foe, and on a model of information conveyance that can speak to every one of the assaults considered in past work; gives a methodical strategy to the era of preparing and testing sets that empowers security assessment; mimicked assault tests can be incorporated into the preparation information to make strides security of discriminative classifiers (e.g., SVMs), while the proposed information model can be misused to outline more secure generative classifiers. We got empowering preparatory comes about on this subject.

Mr .K . SUNDEEP SARADHI

Assistant Professor

"A new test tool for network debugging and faults identification"

Abstract

This paper considers software faults identification along the phases from design to testing and debugging. The following subjects are reviewed and extended: bio-inspired concepts for structuring resilient systems, genetic strategies in test data generation, Ant Colony Optimisation (ACO) algorithms for data flow analyzing and testing, artificial immune systems (AIS) based mutation testing, and fault tolerant approaches inspired by immunity principles in order to increase the software dependability. Data collected during software development cycle can be used to understand the software project evolution and its reliability.

Bio-inspired concepts
The motivation for using bio-inspired methodologies to software development, testing and debugging comes from the requirements of designing resilient software. Some factors that affect the software resilience and the contexts in which programs might run are related to: the complexity level of software systems, the size of infrastructure under interconnectivity, computer network availability and security, the reliability of open source software, the usage of commercial off-the-shelf software, the rate of software renewal (or the retired software), insufficient testing of the reused software etc.

Evolutionary algorithms are population-based meta-heuristic computational solutions inspired by mechanism of biological evolution like reproduction, mutation, recombination and selection. The most related algorithms to the biological models of computing are genetic algorithms that make use of inheritance, mutation, selection, and crossover. However, general evolutionary operators, and recent evolutionary strategies converge to a powerful evolutionary computation paradigm.

Artificial immune strategies

Artificial Immune Systems should offer both innate (predefined) and adaptive (through learning) immunity. Based on clonal selection (CS) theory, proposed by Burnet, the CLONALG is an algorithm proposed by Castro and Zuben , which generates a population on N antibodies, each specifying a random solution for the optimization process (in our case the test planning optimization, test case selection and prioritization etc.), and at every iteration, some of the best (according to a specific metric/fitness indicator) existing antibodies are selected, cloned (proliferated) and mutated to form a new candidate population. The original population is enriched by including a percentage of the best new antibodies, while a percentage of the worst antibodies are eliminated. There are possible many variations of

CLONALG in order to cover some extensions like polyclonal strategies, new immunity operators to prepare the immune response, new learning operators, new

Conclusions

This paper considers software testing phase and investigates on the applicability of nature inspired approaches to test cases generation, test prioritization, and test planning optimization. Software fault identification can be treated as anomalies identification when using artificial immune systems. The software reliability and dependability can be improved by optimized software testing and adequate debugging.

Ms. M. Sri Bala

Sr. Asst. Professor

"Secured Personalized web search using adopted algorithms"

Abstract

Web search engines are valuable tools that are widely used to find specific information in the World Wide Web. When the query is searched in a web should provide the relevant information to the users. The irrelevant results may disappoint the users and the efficiency of the query search should be improved. Personalized web search has established to improve the quality of the various search services on the internet by customizing search results, based on the personal data of user provided to the search engine.

This paper comes with 2 rising trend: internet users wish personalized services and internet users wish privacy. One challenge is that non-public information should be created anonymous beneath the belief that the collaborating parties, together with the online service, aren't utterly sure, owing to a systematic assortment of private info additionally to queries. Another challenge is that the on-line and dynamic nature of cyberspace users. Author planned the notion of online obscurity to guard internet users and planned an approach to bring concern of on-line obscurity through time. This approach makes use of a 3rd party known as the user pool and it doesn't require the user pool to be indisputable. The simulation work of real U.S.A. demographics showed promising results: it's possible to achieve personalization for affordable privacy settings.

An additional privacy live, expRatio, is planned to approximation the number of privacy is endangered to the required min Detail price. However, this paper has been wildcat work on the 2 features: 1st, author modify unstructured knowledge like personal documents, that it's still an open downside on a room to outline privacy. Secondly, the author bridge the conflict wants of personalization and privacy protection by developing the premise on privacy as an absolute customary. Likewise, the writer believes that AN increased balance between privacy protection and search quality are often achieved if the internet search area unit, personalized by providing solely revealing this info associated with a selected question.

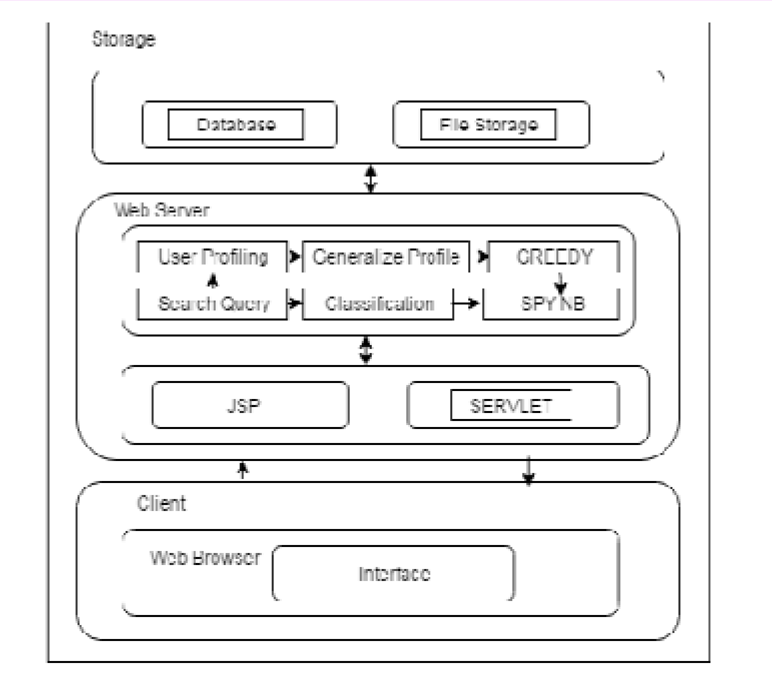


Fig:System Architecture

Algorithms

According to our click through technique, we require to categorize unlabeled data in order to discover the predicted negative urls. Naive Bayes is a simple and efficient text categorization method. However, conventional Naïve Bayes requires both positive and negative examples as training data, while we only have positive examples.

Conclusion:

This paper proposed a client-side privacy protection framework called UPS for personalized web search. UPS could possibly be approved by any PWS that collects user profiles in a hierarchical taxonomy. The framework make users easy users to specify custom-made privacy requirements via the hierarchical profiles. In addition, UPS also functioned online generalization on user profiles to protect the personal privacy without negotiating the search quality. The results also confirmed the effectiveness and efficiency of the solution.

INTERNSHIPS IN ACADEMIC YEAR (2016-17)

Name of the Organisation and Place	Duration From -- to --	No. Of Days	No. Of Students
Anode Info.Tech, Hyderabad	13-05-2016 to 25-06-2016	45	22
BSNL, Vijayawada	13-05-2016 to 25-06-2016	45	1
CITD,MCME, Hyderabad	13-05-2016 to 25-06-2016	45	3
Cyient Ltd, Hyderabad	13-05-2016 to 25-06-2016	45	1
Devmen-IT, Hyderabad	13-05-2016 to 25-06-2016	45	24
Iseef Technologies, Hyderabad	13-05-2016 to 25-06-2016	45	19
Logic Matter, Hyderabad	13-05-2016 to 25-06-2016	45	1
Q-Space, Hyderabad	13-05-2016 to 25-06-2016	45	8
MSMe, Vijayawada	13-05-2016 to 25-06-2016	45	1
Sell.Global Info, vijayawada	13-05-2016 to 25-06-2016	45	14
Satya Tech, Hyderabad	13-05-2016 to 25-06-2016	45	7
NSIC, Hyderabad	13-05-2016 to 25-06-2016	45	3
WebTech.Lab, Hyderabad	13-05-2016 to 25-06-2016	45	10
Y-not SS, vijayawada	13-05-2016 to 25-06-2016	45	2
Vision Tech, vijayawada	13-05-2016 to 25-06-2016	45	1
Naresh.Tech, Hyderabad	13-05-2016 to 25-06-2016	45	1
SNR Investment, Hyderabad	13-05-2016 to 25-06-2016	45	1
Tekcrux pvt Limited, Hyderabad	13-05-2016 to 25-06-2016	45	15
Vision Krest, Hyderabad	13-05-2016 to 25-06-2016	45	1
WebTech.Lab, Hyderabad	13-05-2016 to 25-06-2016	45	7
Web Cognize, Hyderabad	13-05-2016 to 25-06-2016	45	1
		TOTAL	**143**

PLACEMENTS

S.NO	Name of the Company	No of students selected	ANNUAL SALARY (Lakhs)
1	TCS	19	3.36
2	TECH MAHINDRA	08	3.25
3	COGNIZANT	02	3.5
4	FSS	01	3.0
5	ZENQ	04	2.5
6	VEE TECHNOLOGIES	04	2.0
7	VIRTUSA POLARIS	01	3.0
8	EFFECTRONICS	01	2.2
9	JUST DIAL	04	2.28
10	CYIENT	02	3.0
11	ALLSEC TECHNOLOGIES LTD	04	1.2
12	MIRACLE SOFTSYSTEMS	01	1.4
13	ARC SERVE	01	3.36
14	DEEP COMPUTE	01	2.0
15	ALPHABIT TECHNOLOGIES	01	3.0
16	ACCENTURE	01	3.0
17	TAYA TECH	01	3.25
18	TRINITI TECH	01	3.0
19	FISSION LABS	01	3.1
20	INFOSYS	01	3.5
21	CONDUENT	01	3.25

NCC B Enrolment Students

S.NO	RGTL NO	NAME OF THE CADET
1	AP 16 SWA 375532	KOKKILIGADDA TEJESWINI
2	AP 16 SWA 375533	KOTU GOWTHAMI
3	AP 16 SWA 375534	TALLURI VEENA APURUPA
4	AP 16 SWA 375535	CHITIKELA SAMBHAVI
5	AP 16 SWA 375536	POTLACHERUVU ANUSHA
6	AP 16 SWA 375537	BASAVANABOYINA NEHA
7	AP 16 SWA 375538	NALABOLU KAVYA
8	AP 16 SWA 375539	PACHAVA MANASA
9	AP 16 SWA 375540	YERUVADURGA MALLESWARI

SPORTS

S Deepika Got Chess 2nd Place

J Ramya Got Second Place In Athletics

NSS Events

Blood Donation Camp

Inaugaration of Blood Donation Camp by Prasad Reddy Garu

Students Donating Blood

World Health day Activity

Special Camps in Rural Areas.

NSS-UNIT
(National Service Scheme)
SPECIAL CAMP PROGRAMME
8-3-2018 to 14-3-2018
Adopted Village : Pondugala, Mylavaram Ma

Dr K Appa Rao garu delivering a speech to students

Editorial Board

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

TECH-TALK

Biannual Magazine

> "Education is the most powerful weapon which you can use to change the world"

COMPUTER SCIENCE ENGINEERING