Technical Articles

Article-1

Formal Methods in Software Engineering

Software based applications arebecoming ubiquitous in several mission/ safety critical systems and mainchallenge is to provide formalism,techniques and tools to optimize rigordespite system complexity. In safetycritical / mission critical systemsfailure might result in serious impactto an organization and even can causecatastrophes. Rigorous verificationand validation is indispensable.Conventional V&V methods includecode walkthrough/code inspection,static and dynamic testing. However,these traditional methodologies whencarried out rigorously can "Detect thepresence of Bugs" but never "Provethe absence of Bugs". As a practicalalternative, systems / subsystemsneed to be verified with mathematicalproofs termed as "Formal Methods".Formal methods provide a foundationfor special environments leading tomodels that are complete, consistentand unambiguous. Formal methodscan prove "Always or Never" and majorapproaches include Theorem Provingand Model Checking.

Introduction

Formal Methods : Formalmethods are the use of mathematicallyrigorous techniques and tools for thespecification, design and verification of software and hardware systems.By mathematically rigorous wemean specifications are well formedstatements in mathematical logicand formal verification are rigorousdeductions in that logic. The variousphases in which Formal Methods canbe applied to the chosen software are as follows:

Defining Requirements

Modelling: Mathematicalrepresentation of a man-madesystem most suitable for theapplication

Formal Specification:Characterization of an existingsystem expressed in formalspecification language

Formal Analysis / FormalVerification: Model Checking& State Exploration / TheoremProving & Proof Checking

DocumentationThe principal distinction betweenthe two approaches stems from thechoice of formalism used in reasoning process.

Theorem Proving: Theoremproving is one of the key approaches to formal verification. Theorem provingreasons about program P correctness interms of pre and post conditions basedon Hoare Logic, i.e. **{ϕPRE} P {ϕPOST}**.This formula can be read as "if propertyϕ PRE holds before program P starts,ϕ POST holds after the execution of P.In Hoare's calculus, axioms and rulesof inference are used to derive ϕ POSTbased on ϕ PRE and P.These techniques are mostpowerful where properties are written infirst order predicate logic. Correctnessof properties is established through setof stored theorems.

Methodology:

Using formal methods to provethe functional correctness of any logicas per the specifications, a step bystep procedure is mandatory. These steps can be generalised irrespectiveof the techniques used to reasonabout the correctness. Methodology atwork assumes that the model of theimplementation is auto generated bythe tool under consideration and hence modelling the program under test is notconsidered here. The three basic stepsare as follows:

Step 1: *Requirement Analysis*:Detailed requirement analysis isthe first and the foremost importanttask where sound domainknowledge about the system isa pre-requisite. Requirementanalysis can be represented in any semi-formal notation. The outcomeof this step results in identifying the mapping between the input statevector and the expected outputs.This forms the basis to modelformal specifications.

Step 2: *Modelling FormalSpecifications*: This step involvesspecifying the requirementsanalysed in the previous step usingformal notation as per the syntaxand semantics of the specificationlanguage used by the tool under consideration.

Step 3: *Reasoning the correctnessof the code w.r.t the formalspecifications*. Given the codeand the specifications, the toolcarries out reasoning aboutthe correctness of code for its specifications.The subsequent sections describeTheorem Proving and Model Checking techniques with specific tools used.

K. L. Anjali Devi
(13K61A0529)

Aritcle-2

Nano-computing: Perceptible trend and theirApplications

Introduction:

In this innovation-fueled world where nano concept has hovered almost every sphere ranging from thesize of SIM-Cards to the size of gadgets,everyday different approaches are beingresearched and developed to reduce thesize of our computing gadgets and makethem nimbler and efficient towards theenvironment.In early days (mid-1940s) of the invention transistors and IC's were thebase of the digital computers. Digital computers used to be large in size.With the growing years, the accuracy and precision increased whereas thesize decreased. The concept of Nanocomputinghas brought a whole newrevolution in the field of medical, spaceengineering, defense etc. by deliveringhigh end precision devices capableof performing way too intricate andcumbersome processing.

The demand of Nano-computingdevices grew rapidly due to the focus on Portability, Performance and efficiency.

Comparison between Currentand future architecture ofnanotechnology.

CurrentArchitectureFutureArchitectureBoolean logics are usedNeural networks,CNN, QCA...will beused.Binary data representation isusedAssociative,patterned, memorybased etc. data representationswill be used.Based on 2 D Based on 3 DHomogeneous Non homogeneousGloballyinterconnectedNearest neighbour interconnectedSynchronous AsynchronousVon Neumann Integrated memory/logic3 terminal 2 terminal

Perceptible trend in Nanocomputing

Nano-computing is a totally newemerging technology enhancement.Toenhance the computing speeds at tinysizes there are five perceptible trends inNano-computing. They are:

1. Quantum Computing
2. Molecular Computing

3. Biological Computing

4. Optical Computing

5. Nanotechnology Approach

The following sections brieflyexplain these trends and theapplications of Nano-computing.

1 Quantum Computing

Traditional computing is basedon Boolean logic and algorithms. A itis a basic variable having two possiblevalues i.e. 0 or 1 which represent thestate ON or OFF(for 0 it is OFF for 1 it isON). A new approached are introducedthat offers a new set of rules knownas Quantum mechanics. In quantumcomputing the basic variables is knownas QUBIT which is represented in 2DHilbert space as a normalized vector.The implementation of logic withQUBIT is quite different from Booleanlogic, and this opens a lot of possibilitiesand made quantum computing veryinteresting.

The Quantum computer can workwith logic gates having two-mode:XOR [4] and a mode we'll call QO1 (theability to change 0 into a superpositionof 0 and 1, a logic gate which cannotexist in classical computing). If a QUBIThas two aspects than there are foursimultaneous, independent states (00,01, 10, 11); if it has three aspects, thereare eight possible states, binary 000through 111, and so on.

The principles of superposition andentanglement are the two importantrelevant aspects of quantum physics.Quantum computers might proveespecially useful in the followingapplications:

a) Used to Break ciphers

b) Used for Statistical analysis data

c) Used for Factoring large numbers

2 Molecular Computing

Richard Feynman realized that thecell was a molecular machine and atthe molecular level all the informationwas processed.All cellular life is divided into twotypes:

a) Prokaryotes

b) Eukaryotes.

Eukaryotes are those having anucleus like plants, animals, fungi andprotests whereas prokaryotes are thosehaving no nucleus like bacteria.

f. As we know that Bacteria has nonucleus inside so it is unicellular and it is too much smallerthan eukaryotic cells and it isvery difficult to understood incomparison of Prokaryotic cells.Gene is the fundamental unit of allcells.*f*. A gene is made up of informationstorage system known as DNA. *f* DNA is made up of moleculeswhich are known as nucleotides. Each nucleotide contains threegroups i.e. a sugar group,aphosphate group, and a nitrogenbase.Nitrogen bases are basicallyfour types

1) Adenine (A),

2) Thymine (T),

3) Guanine (G) and

4) Cytosine (C).

There are a Hydrogen bondingbetween specific bases i.e. A with T and G with C. DNA encodes information inone strand as a specific sequence of thenitrogenous bases.DNA replication process is notspontaneous as nucleotides arepresent. For the synthesis of nucleotidesand DNA agent are there known asenzymes made up of proteins. Apartfrom this an intermediate moleculenamed as messenger RNA (mRNA) areinvolve in the transformation. By usingTranscription process DNA is convertedinto RNA and translation is the processto generate proteins by using RNA.

3 Biological Computing

In biological computingthe specificity, convenienceand programmability of DNAcomplementarily are exploited.There are two major technicalissues. One is holding and positioningmolecular parts to facilitate assemblyof complex structures and the otherissues are self-replication.The important point of MolecularBiology is to describes how the geneticinformation are inheriting by child fromthe parents which is stored in DNA.

Thegenetic information is used to makesingle copies of that DNA and alsotransferred from DNA to RNA and toprotein.There are two primary approaches:

1) Cellular gates

2) Striker based computation

4 Optical Computing

In the comparison of light, theelectronic signal travels very slow. In 1980s the Optical computing was aheated research area but due to thenon-availability of materials to makeoptical chip the progress goes down. With the limitations imposed by theelectronic components electro-optical devices are available now a day's.

5 Nanotechnology Approach

Nanotechnology is the technologythat deals with dimensions and tolerances of less than 100 nanometers.Especially the manipulation of individualatoms and molecules are done.There are basically two approachesfor synthesis of nano material andfabrication of nano structure:

1) Top-down approach

2) Bottom –up approach

In top-down approach there arecutting of materials in nano size but inbottom-up approach it is self assembly.

Applications

Super computers are enormousin design as well as applications. Supercomputers are very expensivedue to the use of high speed processors and this trait ceases its applicationarea. Nano-computing trend devices

offer similar power, but in a cheap andlight structures. Nano-computing is anemerging field of research.

There arevarious applications of Nano-computing.

1. High performance computing.
2. High-Density inexpensivecomputing
3. Micron scale in-situ computing
4. In Life Sciences, Robotics and Power systems

V Renuka Priya

(13K61A0583)

Article-3

Importance of Secure Coding inMaking "Digital India" Successful

Introduction

Sharp rise of internet and its usagehave commenced a massive digitalproliferation across the world. Theinflux of digital connectivity throughsmart phones and IoT enabled deviceshas carved a new, entirely different"business model" to emerge that isenvironmentally impactful, sociallyeffective, and economically beneficial.Nowadays, people's personalidentifiable information is drifting into adigital form, there by ushering towardsan open and globally accessiblenetwork. Digitization has woven intoour daily life for every single task. Asthat happens, the risks associated withthe digitization has become unnervingand daunting.

The sense of security isa prime concern with every click. As the businesses across the world aretransforming the mode of operation, digital platform is attracting hugevolumes, hence it is imperative thatwe embracerobust security measuresand protections to ensure security ofbusiness operations. Security can beachieved in the digital era by introducingsecure coding in the backstageformulation of digital applications. Overthe last two years, the Indian economyhas witnessed radical enablers whichshall play an important role in takingdigitization into a next level. Some ofthese enablers are:

Demonetization

Recently, on November 8, 2016government of India announced the demonetization of both 500 and 1000 currency notes. As per the government,the demonetization would curtailthe economic imbalance and clampdown the illegitimate and forgedcash transactions in illegal activities. The concept fits well with the view offinancial inclusion and digital Indiainitiative to improve the socio-economicgrowth of marginal sections of society.Again, with the increased usage ofdigital platforms, security is the mainconcern. Because, digital platforms arepotential targets for cyber criminals.With the increased usage of digitalplatform after demonetization, therisks have increased as the followingincidents depict:

f. Fraudulent use of digital paymentnetworks

f. Incidents of data theft

f. Misuse of data

f. Hacking of digital wallets

People want their data to be secureand safe while dealing with digitalplatforms. Therefore, to ensure security,mobile and web application developersneed to include secure coding as aregular practice while developing theapplication.

Digital India initiatives

Digital India evokes the imageof a networked economy that aims to connect over 1.2 billion people acrossthe country. It prepares India for the future Knowledge. Hon'ble PrimeMinister Shri Narendra Modi hasinitiated the Digital India campaignfor transforming India into a digitally empowered technological society.Some of the Digital India initiatives include: mygov.in, digi locker, e-signframework, digitize India platform, national scholarship portal, e-hospital,bharat net, and center of excellence on IoT. With these initiatives, cybersecurity has become the prime concern and forms an integral part of ournational security. The risks associated application vulnerabilities and internetthreats increases as the society is moving towards digitization.

Adoption of secure coding concept

Secure coding must beincorporated in each developmentstage of the web application to provideprotection against cyber-attack,cybercrime, and cyber espionage.Secure coding best practices whenincluded while developing an applicationgives security against the top 10 OWASPvulnerability areas that are:

1. Injection: occurs when a webapplication sends untrusted datato an interpreter as a part of acommand or query.
2. Broken authentication andsession management: occurswhen developers build their owncustom authentication and sessionmanagement schemes that donot consider exhaustive securityconsiderations.
3. Cross site scripting: occurs whenan application takes untrusted data and sends it to a browser withoutproper validation or escaping the input data.
4. Insecure direct object references:occurs when an application uses the actual name or key of an objectfor generating web pages and do not verify the authority of the userwho is accessing the target object.
5. Security misconfiguration: occurswhen secured configuration is not defined and deployedfor application, frameworks,application server, web server,database server, and platform.
6. Sensitive data exposure: occurswhen sensitive data is not encrypted using strong encryption algorithm,not using strong key generation and management method, and notimplementing infallible password hashing techniques.
7. Missing function level excesscontrol: occurs when an application does not protect its functions withproper access control, thereby

allowing access to functionalitywithout proper authorization.

8. Cross site request forgery:occurs when web applicationsallow attackers to predict all thedetails of an action. As browserssend credentials like sessioncookies automatically, attackerscan create malevolent web pages that generate forged requestsappearing genuine.

9. Using components with knownvulnerabilities: occurs whenapplication uses variouscomponents that are not up to date.

10. Unvalidated redirects andforwards: occurs when applicationredirect users to other pages oruse internal forwards.

Significance and Impact

Secure coding is no longer anoption - it is a mandatory concept. It helps in aligning the digital platformsand services as per the best security standard. Some of the key benefits ofincorporating secure coding concepts include the following:

f. It helps in developing secure androbust application that practically reduces the security threats, riskareas, and vulnerabilities

f. It safeguards against the accidentalintroduction of risks to prevent cyber attacks

f. It deploys security controls likeinput validation, access control, data protection, etc. to strengthenthe code from hacking

f. It minimizes development effortsin the Software Development Life Cycle

f. It avoids regulatory penaltiesarising from loss of sensitiveinformation pertaining tocustomers and employeesOne can secure the web and mobile applications by applying the securecoding practices in the development phase.

How can secure coding be the gamechanger?

When included in regular practice, securecoding reduces the vulnerability areas inan application and provides a sense ofsecure transactions with respect to digitalIndia initiatives. Therefore, it is very important to implement robust securecoding concept, which will pave the way for building India strong & stablein the realm of trade & commerce andfor making digital India a successfulcampaign, thereby guaranteeing digital furtherance and India's growth anddevelopment.

G Supriya

(13K61A0524)

Article-4

Security and Geo location

While the increasedpopularity of Videoon Demand (VoD) has givenbroadcasters awealth of newand excitingopportunities to engage consumers, it also bringswith it a host of challenges as viewers expect

access to a full range of video content wherever and whenever suits them. More than ever, consumers are trying tocircumvent geographic restrictions and accessvideo content from all over the world, whethercontent owners consent to it or not. Tools such asVirtual Private Networks (VPNs), Domain NameSystems (DNS), Tor, and proxy servers arehelping drive a growth in the illegal viewing ofgeographically restricted content, posing a significant challenge to the media industry. Andwith the threat of "spoofing" – in which anillegitimate viewer uses technology to impersonatea trusted IP address and appear to have a legitimate connection – having directly affectedthe value placed on content in recent months, the pressure is on to provide and implement robustmeasures to combat the issue.

Where they're hiding

It seems the industry is starting to cometogether in the fight against illegal access, buthow will the new measures affect legitimate,subscription-paying customers?It is important to recognise that not all users who connect to the internet with tools thathide their location are intending to view contentillegally. There are several reasons for connecting via a proxy, for example to protect user privacy,or to take advantage of a faster internetconnection, and ultimately, enjoy an enhancedviewing experience. VPN usage also tends torise dramatically in countries where certain websites are unavailable. For instance, internetusers in China are progressively turning toVPNs to access social networking sites such as Twitter. Increasingly, users are accessingthe internet via mobile connections, evento watch content. However some telcos andmobile providers are sending through centralisedproxy servers, unwittingly changing thecustomer's location.

How to find them

Until now, content operators have understandablyfound the prospect of detecting which usersare illegally viewing content a daunting prospect, as unlike terrestrial channels – whichbroadly speaking do not function outside theircountry of origin – digital channels require adifferent approach and a clear strategy forhandling geofencing.IP geolocation technology, however, enablesbroadcasters to pinpoint where in the world a useris viewing content, right down to their postcode.Once the viewer's location has been established,the broadcaster can decide whether to allow orrevoke access to that user depending on thecountry they are in. In many cases, geo detectiondown to a postcode level may be overkill but inreality, with geographic borders being just a lineon the map, country-level accuracy has becomeincreasingly important. Recognising when a Norwegian subscriber drives into Sweden andmay only be a few miles away from his or herhome address is a big concern for many VoD

channels. This level of "bleed" used to be deemedacceptable within the streaming space, but withtighter margins this is no longer the case.

Layering on proxy knowledge to understand thosewho may knowingly (or not) be changing theirphysical locations can keep broadcasters on the right side of their geofencing commitments.

IP intelligence and geolocation at work

One company that has successfully incorporatedIP intelligence and geolocation data into its digitalrights management (DRM) initiatives is VUBIQUITY. The organisation connects contentowners and video providers to deliverentertainment to viewers on any screen, andworks with nearly 650 leading film studios,television networks, independent producers andmulti-channel networks (MCNs) to bringpremium content to over 1,000 global videodistributors spanning 109 million householdsacross 121 territories.VUBIQUITY needed to find an IP geolocationprovider that would offer accurate and reliabledata, specifically for African and Latin Americanregions, to gain access to high quality, allencompassingdatasets that were continuallyupdated. Using IP intelligence technology, the company was able to uncover actionableinformation about online users such as geographiclocation and proxies (including VPNs) – all while respecting the user's right to privacy.

According toVUBIQUITY, the risks are significant without this type of digital protection and the companytakes comfort in knowing that it is using reliable,quality data to meet the studios' licensingrequirements, protecting not only the studios,but also the company and its operators.

Restoring value for content producersand distributors

To optimise revenues, the media industry mustconstantly adapt to changing consumer habitsand the growth of digital platforms, whichpresent wider opportunities to connect. AnalysingIP addresses is a complex business, with newattempts to overcome restrictions occurring on adaily basis. Winning this game of "whack-a-mole"requires expert engineering knowledge and regularupdates 365 days a year. Meanwhile, isolatingsuspect connections means the rest of the userbase (i.e. legitimate customers) remainsunaffected, and media companies are able toprotect the value and revenue derived frompremium content, which would otherwise be lostto opportunistic proxy users taking advantage ofmodern-day technology.

How to find them

Until now, content operators have understandablyfound the prospect of detecting which usersare illegally viewing content a dauntingprospect, as unlike terrestrial channels – whichbroadly speaking do not function outside theircountry of origin – digital channels require a

different approach and a clear strategy forhandling geofencing.IP geolocation technology, however, enablesbroadcasters to pinpoint where in the world a useris viewing content, right down to their postcode.

IP intelligence and geolocation at work

One company that has successfully incorporatedIP intelligence and geolocation data into its digitalrights management (DRM) initiatives is VUBIQUITY. The organisation connects contentowners and video providers to deliverentertainment to viewers on any screen, and works with nearly 650 leading film studios,television networks, independent producers andmulti-channel networks (MCNs) to bring premium content to over 1,000 global videodistributors spanning 109 million householdsacross 121 territories.VUBIQUITY needed to find an IP geolocationprovider that would offer accurate and reliabledata, specifically for African and Latin Americanregions, to gain access to high quality, allencompassingdatasets that were continually updated.

Restoring value for content producersand distributors

To optimise revenues, the media industry mustconstantly adapt to changing consumer habitsand the growth of digital platforms, whichpresent wider opportunities to connect. AnalysingIP addresses is a complex business, with newattempts to overcome restrictions occurring on adaily basis. Winning this game of "whack-a-mole"requires expert engineering knowledge and regularupdates 365 days a year. Meanwhile, isolating suspect connections means the rest of the userbase (i.e. legitimate customers) remainsunaffected, and media companies are able toprotect the value and revenue derived from premium content, which would otherwise be lostto opportunistic proxy users taking advantage ofmodern-day technology.

Focusing on high-quality data – powered byaccurate IP intelligence and geolocationinformation – will enable media companies tostrike that all-important balance betweencompliance with geographical rights and provisionof a first-class streaming service, which keepstheir customers coming back for more.

K H Indira Devi
(13K61A0538)