

National Centre of Excellence
for Cybersecurity Technology
Development & Entrepreneurship

DSCI
PROMOTING DATA PROTECTION
A **NASSCOM**® Initiative

A JOINT INITIATIVE BY



**Ministry of Electronics &
Information Technology**
Government of India

VIRTUAL ROADSHOW ON

India's Cybersecurity R&D Capability

*Unlocking the Growth of Indian
Cybersecurity Ecosystem*



Exhibitor Handbook

About National CoE

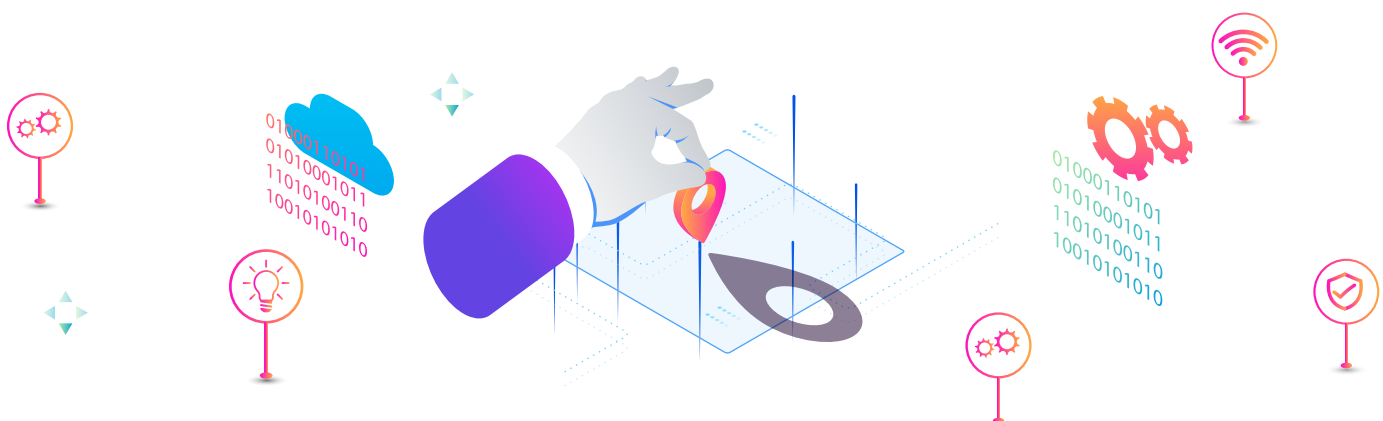
The National Centre of Excellence for Cybersecurity Technology Development is a joint initiative conceptualized by the Ministry of Electronics & IT (MeitY) and DSCI for setting up connected, concerted & coordinated efforts to catalyse and accelerate cybersecurity technology development and entrepreneurship in the country. NCoE is working to establish India as a leading hub for cybersecurity capabilities and leverage the expertise to secure the Digital India of Tomorrow from cyber threats.

The purpose of this national effort was designated as *“To establish India as a leading hub by accelerating identification and development of cyber security technologies in the country to further strategic objectives, develop critical capabilities, exploit commercial potential, and thereby driving future readiness.”*

About Event

The giant leaps in digital technology development have created a new arena to embolden the Cybersecurity landscape of our nation. India is now at the forefront of Cybersecurity R&D, in terms of people, process, and technology. To elevate India's posture in the Cybersecurity R&D and to promote productization, commercialization, and increasing industry adoption of the cybersecurity research work in the country; National CoE is hosting first-of-its-kind 'Cybersecurity R&D Roadshow'.

The roadshow will bring the Academia, R&D Institutes, and Public Sector together to leverage Cybertechnology Development and Entrepreneurship Ecosystem in the country, and it will offer a unique platform to them to showcase their latest research and development work in the area of cybersecurity.



Agenda

10:15 to 11:00

INAUGURAL

Welcoming Address Ms. Rama Vedashree CEO, Data Security Council of India	Inaugural Address Dr. Rajendra Kumar Additional Secretary, MeitY	Special Address Lt Gen (Dr) Rajesh Pant National Cyber Security Coordinator
--	---	--

11:00 to 11:45

PLENARY SESSION

Cybersecurity R&D: Scaling up for India's Future Readiness

Mr. Arvind Kumar Scientist G and Group Coordinator, Cybersecurity RnD, MeitY	Dr. S D Sudarsan Executive Director, C-DAC	Dr. Sachin Lodha Principal Scientist, TCS Research and Innovation
--	---	---

Chair: Dr Gulshan Rai, former National Cyber Security Coordinator

11.45 to 12.00

PRESENTATION

Multiplying the efforts in Cybersecurity R&D
 National CoE, a join Initiative of DSCI and MeitY
 Mr. Vinayak Godse, VP, DSCI

12.00 to 13.00

EXHIBITION

Explore the Country's R&D Capabilities and Work Exhibition Time 12:00 to 13:00	Next Generation Network Security BARC's R&D program in Electronics, Control, Instrumentation and Computers Mr. Gigi Joseph, Chief Information Security Officer, Bhabha Atomic Research Centre 12:00 to 12:20	Leading Public Sector Cyber Security R&D Effort Cyber Security R&D of C-DAC Dr. Subramanian Neelakantan, Senior Director (R&D), C-DAC 12:20 - 12:45	Leading Public Sector Cyber Security R&D Effort Cyber Security R&D of CSIR Dr. GK Patra, Principal Scientist, CSIR 12:45 - 13:05
---	--	---	--

NETWORKING TIME 13:00 to 14:00 EXHIBITION TIME

14:00 to 15:00

PARALLEL TRACK

Use Cases and Opportunities of Cyber Security R&D
 IoT/Hardware, Cloud, Quantum, 5G, Automotive

Dr Bresh Lall, Professor, Electrical Engineering Department, Former coordinator Ericsson 5G CoE, IIT Delhi	Dr Debdeep Mukhopadhyay, Professor, Computer Science and Engineering, IIT Kharagpur	Mr. Anand R Prasad, Founder and CEO, Wenovator LLC	Shri Narendra NathGangavarapu, Joint Secretary, NSCS, Government of India
--	---	--	---

Moderator: Mr Vinayak Godse, VP, DSCI

14:00 to 15:00

PARALLEL TRACK

Cyber Collaboration: Industry, Start-up & Academia
 Case studies of how this has worked

Dr Chittaranjan Hota, Professor, Computer Science and Engineering Department, BITS Pilani - Hyderabad	Mr Vivek Shenoy, CTO, QNu Labs & Angel Investor	Mr Meenu Singhal, Vice President, Industry - Automation Business, Schneider Electric
---	---	--

Moderator: Mr Sivarama Krishnan, Partner and Leader, Cyber Security, PwC India



Agenda

KEYNOTE

Special Keynote on India Cybersecurity RnD

Mr. Ajay Prakash Sawhney, Secretary, MeitY

15:00 to 15:15

EXHIBITION

Explore the Country's R&D Capabilities and Current Research Projects

Exhibition Time

Dr. P. Sateesh Kumar,
Associate professor,
Computer Science and
Engineering, IIT Roorkee

Dr. Deepak Garg,
HOD and Professor, Computer
Science Engineering, Bennett
University

Prof. Gaurav Varshney,
Assistant Professor,
Computer Science and
Engineering, IIT Jammu

15:15 to 16:15

SESSION ON

Making India a Global Hub for Security R&D and Product Entrepreneurship

Prof. V. Kamakoti,
Professor, Department of
Computer Science, IIT
Madras

Ms. Jhilmil Kochar,
Managing Director, CrowdStrike,
India

Mr. Vikram Gupta, Founder
and Managing Partner,
IvyCap Ventures

Moderator: Rama Vedashree, CEO, DSCI

16.30 to 17.15

EXHIBITION

Explore the Country's R&D Capabilities and Current Research Projects

Exhibition Time

17.15 to 17.45



Exhibitors Logo





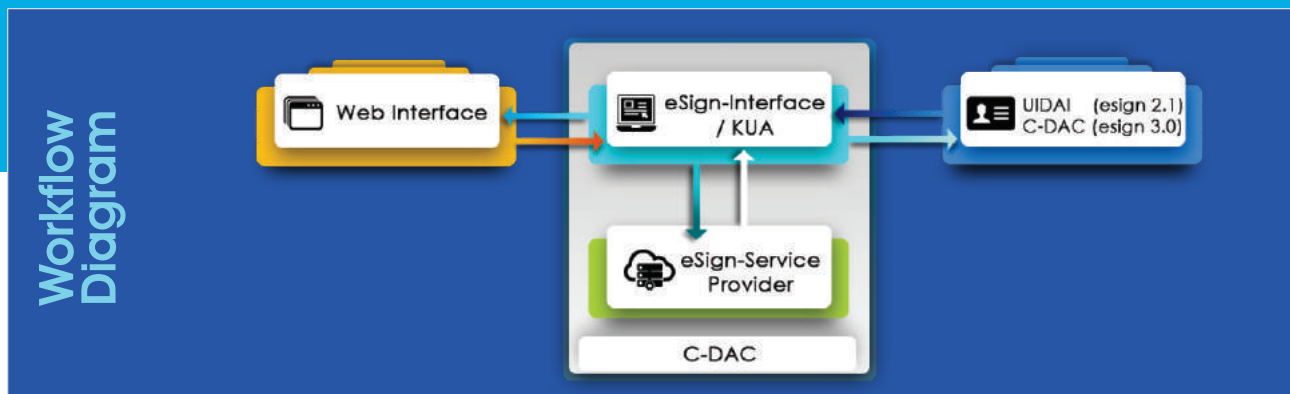
सी डैक
CDC

BOOTH 01



C-DAC's On-line Digital Signing Service

Imagine a life without carrying a pen and no printed application forms required to be filled in, for opening an account in a bank or for getting a PAN card. It was the signature put by applicant on the form that was preventing them from going online. But now, it is possible to replace hand written signature by electronic signature, which can be put in documents in electronic form. C-DAC offers a service called eSign that will allow citizens to sign documents electronically, thereby saving time and efforts for them.



Benefits of e-Hastakshar: C-DAC's online Digital Signing Service

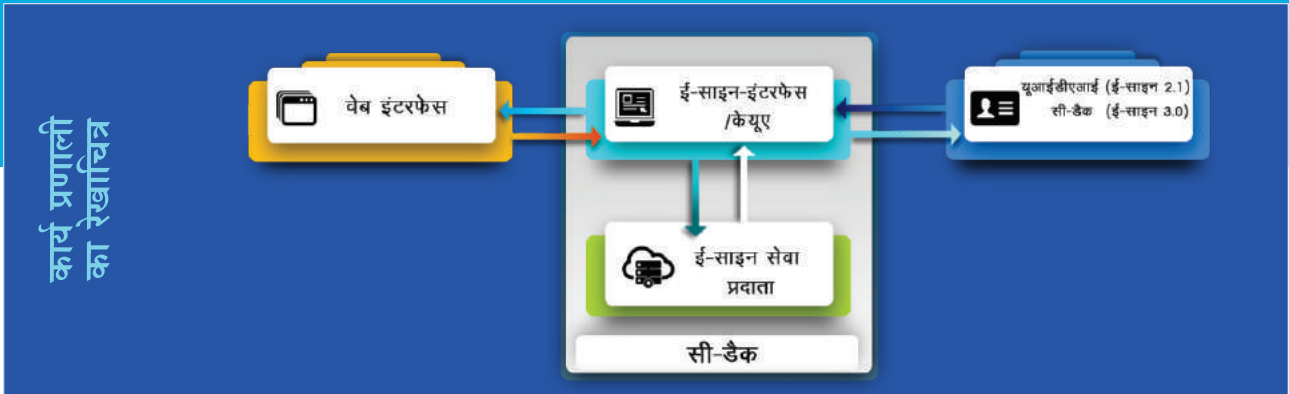
- Time and cost effective
- Easy and secure way to digitally sign at anywhere, anytime
- Facilitates legally valid signatures
- Flexible and easy to implement
- Secure online service
- OTP/Biometric based authentication for Aadhar eKYC
- Two factor authentication (OTP with PIN) for C-DAC eKYC
- Provides legally valid signatures as per Indian IT Act 2000
- Using open API facilitates applications to leverage digital signature service
- Ensures privacy of users by requiring only the thumbprint (hash) of the document for signature instead of whole document
- C-DAC follows the guidelines of CCA and Aadhar to provide security
- C-DAC is an empanelled eSign service provider (ESP) and a Certifying Authority (CA)

Applications

- [e-Governance](#)
- [Citizen Services](#)
- [Office Automation](#)
- [Digital Locker](#)
- [Education Sector](#)
- [Transport Sector](#)
- [Financial Sector](#)
- [Passport](#)
- [Telecom](#)
- [Tax Sector](#)

सी-डैक की ऑन-लाइन डिजिटल हस्ताक्षर सेवा

कल्पना कीजिए कि हमें बैंक में खाता खोलने के लिए या पैन कार्ड पाने के लिए न कलम की आवश्यकता हो और न ही आवेदन प्रपत्रों को भरने की। इन प्रपत्रों पर आवेदक के हस्ताक्षर की आवश्यकता के कारण ऑनलाइन करने में एक कठिनाई होती है। लेकिन अब इलेक्ट्रॉनिक हस्ताक्षर के द्वारा हस्तलिखित हस्ताक्षर की आवश्यकता बदलना संभव है। यह नए हस्ताक्षर इलेक्ट्रॉनिक रूप में दस्तावेजों में संलग्न किए जा सकते हैं। सी-डैक की ई-हस्ताक्षर नामक सेवा, इन प्रयासों को सरल बनाती हैं और अब नागरिक इलेक्ट्रॉनिक माध्यम से ई-हस्ताक्षर कर सकते हैं।



ई-हस्ताक्षर के लाभ: सी-डैक की ऑन-लाइन डिजिटल हस्ताक्षर सेवा

- समय और लागत प्रभावी
- कहीं भी, कभी भी डिजिटल रूप से हस्ताक्षर करने का आसान और सुरक्षित तरीका
- कानूनी रूप से वैध हस्ताक्षरों की सुविधा
- कार्यान्वित करने में आसान
- सुरक्षित ऑनलाइन सेवा
- आधार ई-केवाईसी के लिए ओटीपी / बायोमेट्रिक पर आधारित प्रमाणीकरण
- सी-डैक के ई-केवाईसी के लिए दो कारक (फैक्टर) प्रमाणीकरण (पिन के साथ ओटीपी)
- भारतीय आईटी अधिनियम 2000 के अनुसार कानूनी रूप से वैध हस्ताक्षर
- मुक्त प्रारूप की एपीआई के कारण एप्लीकेशन का सहज प्रयोग
- उपयोगकर्ताओं की गोपनीयता की आश्वासना के लिए पुरे दस्तावेज के बजाय केवल हैश (Hash) की आवश्यकता
- सुरक्षा प्रदान करने के लिए सीसीए और आधार के दिशानिर्देशों का सी-डैक द्वारा पालन
- सी-डैक एक पंजीकृत सीए (CA) एवं अनुमोदित ई-हस्ताक्षर सेवा प्रदाता (ESP) है

एप्लिकेशन्स

- ई-गवर्नेंस
- नागरिक सेवाएं
- ऑफिस ऑटोमेशन
- डिजिटल लॉकर
- शिक्षा विभाग
- परिवहन क्षेत्र
- वित्तीय विभाग
- पासपोर्ट
- दूरसंचार
- कर विभाग



Blockchain based Proof of Existence as a Service (PoEaaS)

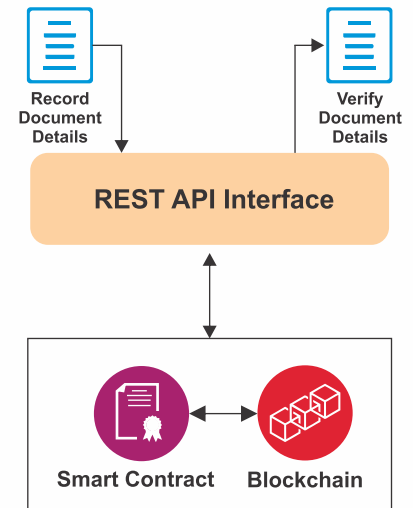


About Blockchain

Transparency, security and efficiency are important requirements in digital society. Blockchain is one of the emerging technology, which plays a significant role in enabling these requirements. Different departments generate a number of digital artefacts such as Educational Certificates, MoUs / Agreements, Driving licenses, Health Records, Employee Service Records, Sale Deed & Property Registration Records, Birth & Death certificates, Tax returns and so on. Important aspects associated with these documents are temporal existence, origin and content authenticity. C-DAC has developed a Blockchain based platform for Proof-of-Existence of documents, which would be offered as a service.

What is Proof Of Existence (PoE)?

PoE calculates the cryptographic digest of digital artefact and stores in the Blockchain along with the timestamp. It allows verifying the existence of digital artefact's hash on the blockchain. This proves the existence of digital artefact at a point of time when it was recorded on blockchain. The key advantages of PoE include anonymity, permissioned verification, privacy, and getting a decentralized proof which is difficult to tamper.



Benefits of PoE

1

Proves document Ownership without revealing actual data

2

Record time stamp & proves digital artefact exists at a certain moment of time

3

Certify the existence of document without the need of a Central Authority

4

Ensures document Integrity

5

Ensures that timestamp and hash of the documents cannot be tampered retroactively

Upload Document for Proof-of-Existence

No file chosen

Latest documents registered on Blockchain

Transaction ID	Hash	Status
33064fed224d4aef6405....	de676a0844bfb5cae59d...	Success
672c3f227078541d8bcf...	343c8e11568eb1ffa708..	Success

Search for document existence
Use document hash or transaction ID for search


OR

This platform records details of digital artifacts in a tamper proof manner. After recording the details, a receipt with embedded QR code will be generated and provided for further verification. This facilitates in proving that the digital artifacts were created on a particular date & time along with the authenticity of the document contents and its origin.

PoE Receipt

Transaction ID:	0287684c2353f50e55dff90bde151cc027f6ff5d226312ab6b7a0519bb73b7c0
File Name:	0287684c2353f50e55dff90bde151cc027f6ff5d226312ab6b7a0519bb73b7c0.pdf
File Type:	application/pdf
Document Type:	Property Document
Issuer User:	Manish
Issuer Organization:	CDAC
Issuer to:	Manish
SHA256	0ea52d3d01d43234765a5a61e6f785e76e30741da1989b3cee18b4091695d646
Status:	Success
Registration Date:	Fri Nov 16 2018 18:14:47 GMT+0530 (IST)

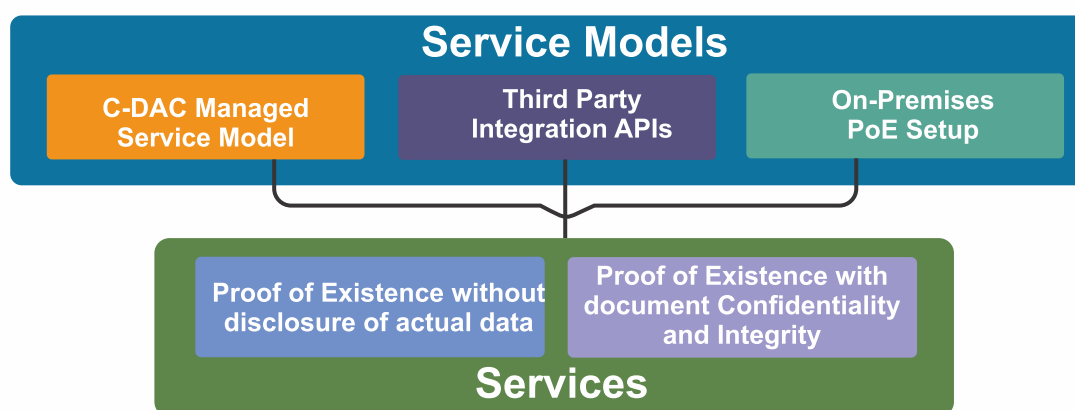
<http://cdacchain.in>
 Scan QR-Code or visit above url to verify authenticity of this document.
 This document is computer generated and hence does not require signature



Potential Use Cases of PoE

- Educational applications: Publishing of educational transcripts and certificates that are verifiable during the recruitment process.
- E-Governance applications: Proving the existence of sale deed linked to the time during the property registration process, storing and verification of birth/death certificates by third parties and so on.
- Enterprise Document Management: Recording important documents generated over the time in an enterprise and its verification during the audit .

PoE Service Models



For demo and queries mail us at cdacchain@cdac.in



प्रगत संगणन विकास केन्द्र

CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार

A Scientific Society of the Ministry of Electronics and Information Technology, Government of India

Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisaillam Highway, Pahadi Shareef Via (Keshavagiri Post) Hyderabad - 501510



सी डैक
CDC

BOOTH 02





e-Pramaan

SSO and e-Authentication Solution

e-Pramaan is an e-Authentication framework, which facilitates authentication and security of users accessing various services on mobile and fixed platforms. It is a unique mechanism providing unified log-in facility through SAML 2.0 based Single Sign-On (SSO) for integrated services. The Single Sign-On feature provides registered users a single window access to all services that are integrated with e-Pramaan.

e-Pramaan offers following multi-factor authentication:

- **Password:** Text Password and/or Image Password
- **One Time Password (OTP):** Mobile, e-Mail and/or Mobile App
- **Digital certificate:** DSC with Indian CA
- **Biometrics:** Fingerprint and IRIS (Currently Aadhaar based)

Features of e-Pramaan:

- **2-way authentication:** assures the user about the authenticity of service URL reducing the possibility of phishing attacks.
- **Identity proof verification:** based on PAN, Driving Licence or Aadhaar No. This helps to map a virtual identity to a real one.
- **Multi-device multi-platform support:** available in Java, Dotnet and PHP
- **Flexible authentication chaining schemes:** departments can choose various combinations of authentication types and change this at runtime.
- **Mobile Application:** Android app available at the government appstore <https://apps.mgov.gov.in>
- **Seamless migration to upgraded authentication techniques:** departments can upgrade to new authentication factors at runtime.
- **First Level Authorization:** Departments have the provision to map users to roles

All the above features enable the departments in imparting more data sensitive services to rightful users.

e-Pramaan is currently provided as a service and solution both. The components of e-Pramaan like OTP service, Digital certificate based authentication can be availed individually as per the requirements.



SSO and e-Authentication Solution



- Password
- One Time Password (OTP)
- Digital Signature Authentication
- Biometric

“ e-Pramaan is a uniform standard based national e-Authentication framework to authenticate users of various government services in a safe and secure manner for accessing services through desktop as well as mobile. ”



Contact Details:

<https://www.epramaan.gov.in> | <https://authenticate.epramaan.gov.in> | <https://department.epramaan.gov.in>

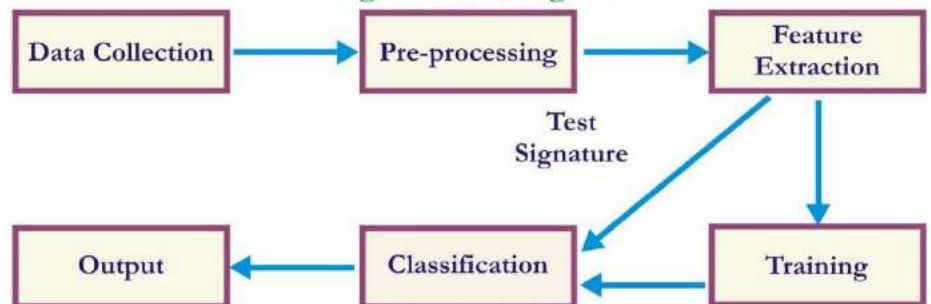
Online Signature Authentication System

Automatic Online Signature Verification/Identification

Automatic Handwritten Signature Verification/Identification system, is one of the most powerful and acceptable means of personal authentication available, with a wide range of applications in industries, public and health sector, R&D labs and many more. This behavioural biometric system provides a robust, user-friendly, language independent solution capable of verifying human identity.



Program Flow Diagram



Applications

Authentication of individuals is rapidly becoming an important issue due to increase in identity fraudulence. Online signature verification has a wide range of applications in the field of access control, R&D labs, POS applications, Forgery detection, branch automation, Money withdrawal from ATM, check processing and restricted access in savings bank accounts in banks etc.

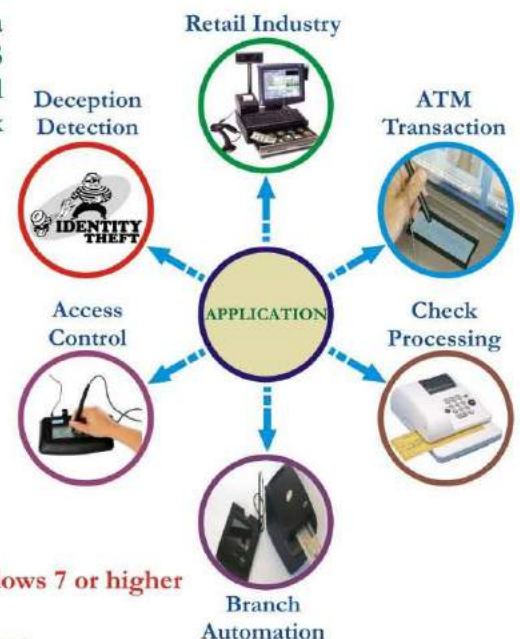
Features of Online Signature Verification System

- Language independent solution, capable of processing dynamic features of the handwritten signature
- Enrolment, training of signatures along with verification are bundled into one place
- Ease of use, seamless handling with a rich blended graphical user interface
- Dynamic signatures are saved in image files automatically
- Print option for signatures is facilitated for record keeping purpose
- Acceptable recognition/verification accuracy in genuine cases

Software Requirements

Operating System: - Windows XP with Service Pack 3, Windows Vista, Windows 7 or higher

Driver: - Wacom Intuos 5 Windows Driver 6.3.7-6 (XP, Vista, Win 7, Win 8)



Online signature data collection interface



Signature verification Interface

Hardware Requirements

Intel® Pentium® 4 or AMD Athlon® 32/64 bit processor (2 GHz or faster)
 4.65 MB of available hard-disk space for installation; additional free space required during installation
 Minimum 1 GB of RAM (2 GB Recommended). Works with Wacom Intuos 3/5 tablet with stylus, Wacom STU series signature pad or Tablet PC etc.



ICT & Services Group:

प्रगत संगणन विकास केन्द्र

CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Plot - E2/1, Block - GP, Sector - V, Salt Lake City, Kolkata - 700091, INDIA

Tel: +91-33-2357 9846/5989 (Ext. 216), 91-33-2357 4258 (Direct), Fax: +91-33-2357 5141, Website: www.cdackolkata.in

For further details contact: Shri Asok Bandyopadhyay, e-Mail: asok.bandyopadhyay@cdac.in or

Dr. Amit Chaudhuri, e-Mail: amit.chaudhuri@cdac.in



सी डैक
CDC

BOOTH 03

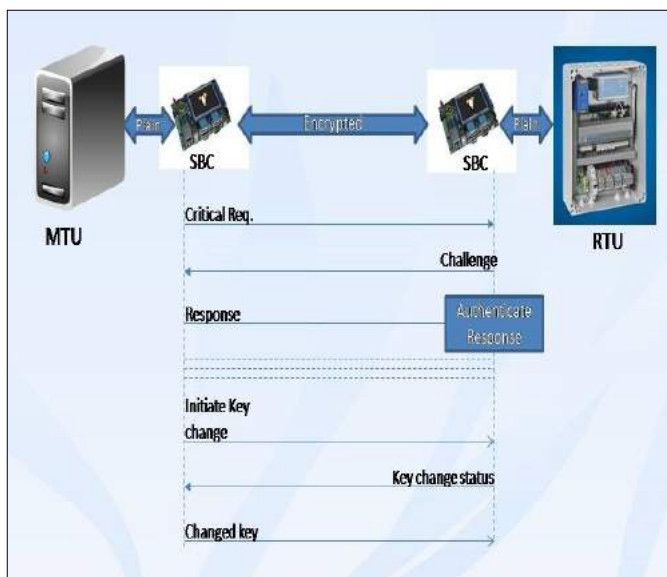
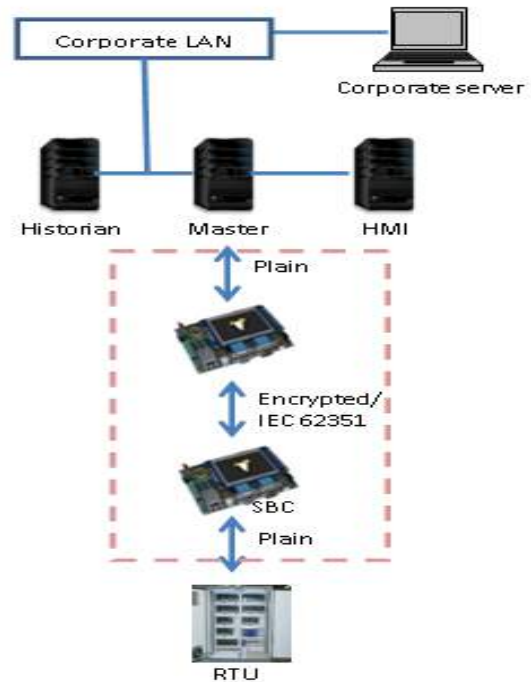


About Product

C-DAC's COPS Defender is a protocol hardening solution intended to address the vulnerabilities in transmission SCADA protocols like IEC 60870-5-101 and IEC 60870-5-104 in the power systems. The solution offers to authenticate any control from the control center towards RTUs and prevent any malicious events that may take place due to man-in-the-middle attacks. This also provides an encrypted channel between a control center and the RTUs connected to it. This is aimed to address the security concerns like data spoofing, data modification, replay attack and non-repudiation.

Features

- Hardening of the following protocols:
 - IEC 60870-5-101
 - IEC 60870-5-104
- Deployable with existing SCADA environment
- Implements encrypted channel between RTU and control center.
- Adherence to IEC 62351 standard for providing application layer security.
- Identifying possible man-in-the-middle attack and preventing consequent attacks like data spoofing, data modification and replay attack.



Product Highlights

- Product field tested at Karnataka Power Transmission Corporation Limited (KPTCL), Bangalore and Southern Regional Load Despatch Centre (SRLDC), Bangalore.
- Highly interoperable due to the strict adherence to the standards.
- Tolerable impact on the response times.

Product Details

- Adopting Bump In the Wire methodology to protect third party Master Terminal Unit and Remote Terminal Unit
- Application layer security adhering to IEC 62351 standards
- Secured mutual authentication
- Protects communication channel between RTU and MTU
- Encryption of data over communication channel
- Secured key exchange
- Prevents various attacks like Man in the middle, Replay, Data Modification, Non Repudiation etc.
- Latency within limits

About Product

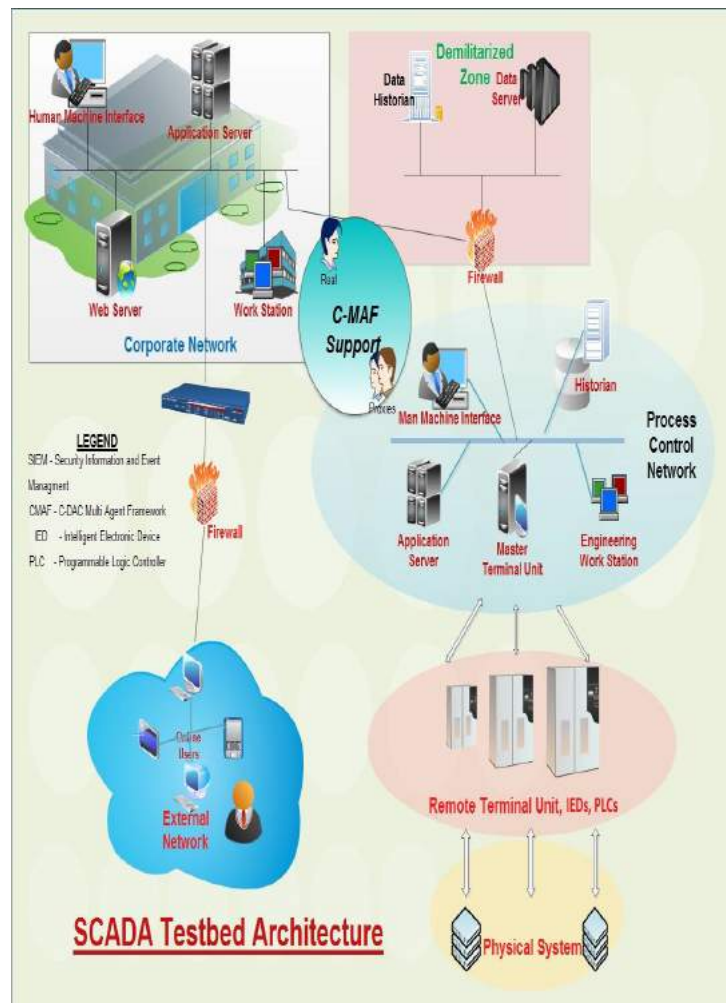
Supervisory Control and Data Acquisition (SCADA) Testbed is modeled in defense-in-depth architecture and used to simulate attacks. Testbed can be used to assess the vulnerabilities and analyzing the impact of attacks on the performance and availability of SCADA systems. Multi agent based framework (CMAF) has been used for simulation as well as administration. SCADA Testbed is provided with tools such as SCADA Threat Analyzer (STA), Security Information and Event Management (SIEM) and Testbed Management tool. STA tool can be used to simulate and analyze the attack scenarios, SIEM tool can be used for continuous monitoring of attack and Testbed Management tool can be used for management/ diagnosis of whole testbed.

Features

- A complete attack simulation, monitoring and management environment.
- Provides tools such as SCADA Threat Analyzer, SIEM and Testbed management.
- Employs C-DAC's Multi Agent based deployment Framework (CMAF) without impacting SCADA System reliability.
- Efficient Analysis through SCADA Threat Analyzer
- Uses correlation, data aggregation, and retention for anomaly detection and forensics investigation.
- Testbed management tool used for starting/stopping services as well as monitoring the healthiness.
- SIEM tool provides real time dash board of events

Product Details

- Real time simulation of attacks in a controlled environment
- Scalable architecture
- SCADA testbed follows Live, Virtual and Constructive (LVC) model.
- Automation for conducting attacks and monitoring over the network with standard in-house CMAF implementation.
- Instant retrieval of experimental results history.
- STA tool Integrates key features like network monitoring, process monitoring, file monitoring, memory monitoring, signature based file scanning, for in-depth analysis of different attack scenarios.
- STA tool provides Operational Dashboard for analyzing all possible parameters on a single window.
- SIEM tool provides features such as monitoring operating system events, application events, updating on real time dash board and archiving the events for forensics.
- Testbed management tool provides features such as starting/ stopping of services of all systems, monitor and diagnosis of whole testbed health status.





SCADA Protocol Anomaly DEtector



SPADE

Passive Security Monitoring Solution

About Product

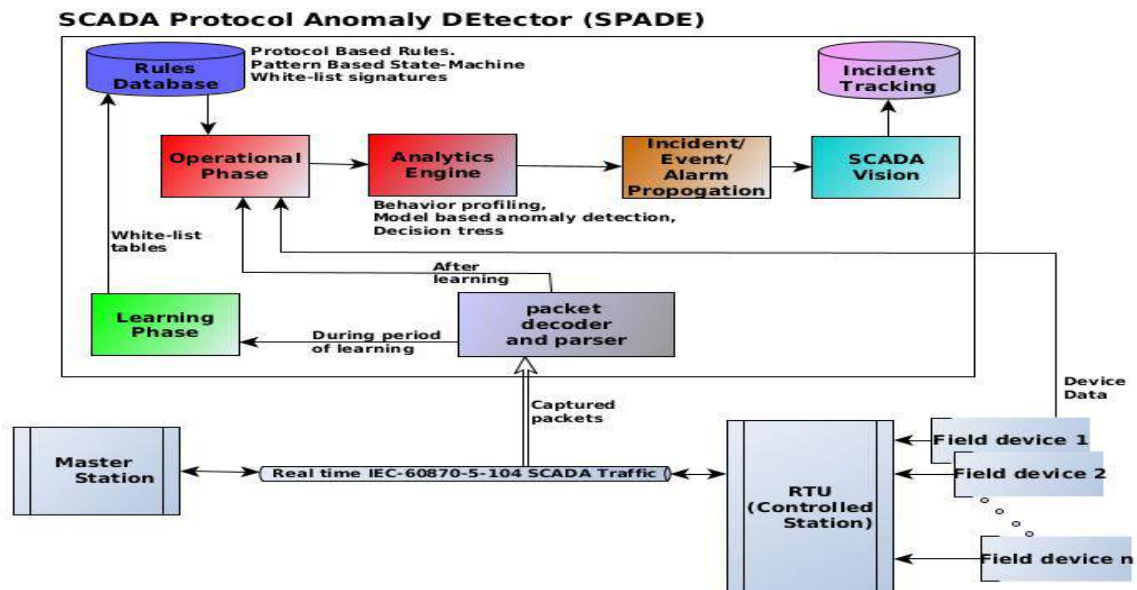
C-DAC's COPS SPADE (SCADA Protocol Anomaly Detector) is a passive security monitoring solution targeting at the security of remote terminal units (RTU). SPADE actively detects anomalous communication (between RTU and master) and works on deep packet inspection (DPI) and deep content inspection (DCI) based analytics engine. Analytics engine is based on white-listed rules and modeled specifically for IEC-60870-5-104 based SCADA systems. Along with the white-listed rule sets, the solution includes field (sensor/actuator values) data correlation with network data. SPADE can detect known and unknown zero-day attacks on the SCADA systems effectively.

Features

- Plug-in solution without affecting architecture of the existing system
- Does not interfere with operation of the existing system
- Attached in parallel to RTUs in the same network
- Can capture zero day attack scenarios
- Single dash board (SCADA Vision) at control centre to monitor status of all RTUs
- Operate in promiscuous mode
- Failure of this solution does not affect the real time operations
- Can be deployed whether RTUs are modern/legacy/ proprietary
- Monitor all communication between RTU and master, detect and report any abnormalities/attacks at RTU
- SMU analyzes exchanged messages and commands initiated from master to perform integrity checks, detect any suspicious events.
- Detect attacks on RTU such as DoS, malfunctioning of RTU/master, brute-force attacks, zero day attacks.

Technical Details

- SPADE works on two phases i.e. learning phase and operational phase
- Learning phase is to prepare white list tables based on meta data and uniform data classification
- In operational phase, SPADE sniffs real time data and applies DPI/ DCI methodologies with support of protocol based rule sets, pattern based state machines and provide these results to analytics engine
- Analytics engine works based on behavior profiling, decision tress, model based anomaly detection and generates alarms/ events/ incidents based on risk level
- Takes a separate feed of sensors raw value without affecting RTU operations to detect anomalies
- SCADA vision is a geo location based real time dash board with incident tracking and risk prioritized alarms/ events/ incidents support.



Center for Development of Advanced Computing

Real time systems & Internet of Things (RTS&IoT)

C-DAC Knowledge Park, No:1, Old Madras Road,

Byappanahalli, Bangalore. Ph: +91-80-25093400/12

Contact Person: Rajesh Kalluri, Mob: 9886917196



INFORMATION SECURITY EDUCATION & AWARENESS - PROJECT PHASE - II

Keeping in view the pervasive nature and impact of cyber security on all walks of life - economic and social, Government of India has identified Information Security as one of the major thrust areas for launching various developmental programs. One of the key elements essential for information security is availability of right kind of qualified and well trained human resource, development of indigenous solutions / software and secure maintenance of critical infrastructure of the country.

Ministry of Electronics and Information Technology (MeitY) has approved a project in 2005 entitled Information Security Education and Awareness (ISEA) which was completed in 2014 and Phase II of the said Project was approved in April 2014 with an outlay of Rs. 97.04 crore for a period of 5 years.

Areas of Coverage

Academic Activities:

1,14,038 persons to be trained under formal & non formal courses, faculty training etc. Besides this, around 400 paper publications are expected from ISRDCs, RCs, PIs

Training of Government Personnel :

13,170 officials in five years

Creation of Mass Information Security Awareness towards academic, general and Government users covering approximately 3 crore Internet users either through direct or indirect mode

Implementation Structure

The implementation of the ISEA Project Phase-II is carried out through the following:

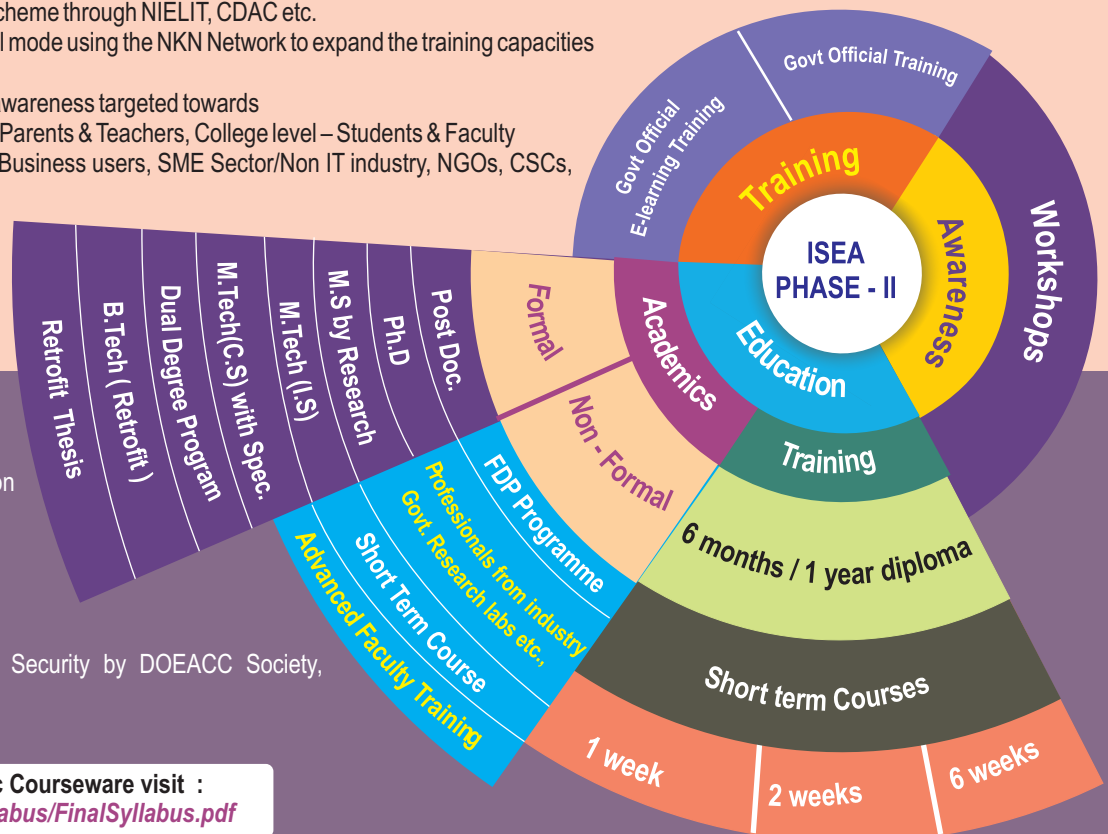
- Fifty one (51) Institutions for academic activities:
 - Information Security Research and Development Centres (ISRDC) - 4
 - Resource Centers (RCs) - 7
 - Participating Institutes (PIs) - 40, in three categories
- Sixteen (16) Implementing Agencies for training of Government Officials with one coordinating agency i.e. NIELIT Centre Gorakhpur
- Awareness programs through Implementing Agencies, PIs, RCs, etc., with one coordinating agency i.e. C-DAC Hyderabad
- An Institutional Mechanism / Program Management Unit (PMU) has been set up at C-DAC Hyderabad

Objectives

- Capacity building in the area of Information Security to address the human resource requirement of the country, by
 - Generation of core research manpower to undertake basic/fundamental research, applied research, research in the area of product/solution design and development and in selected thematic areas of national strategic importance to build indigenous capability
 - Introduction of Information Security curriculum in formal courses like M.Tech./M.E./M.S., B.Tech/B.E., Post Graduate Diploma courses, faculty training, modular/short term knowledge oriented courses etc. through academic institutions
 - Launching non-formal modular/short-term knowledge-cum-skill oriented courses etc. for working professionals at all levels including the flexible certificate programs, certification scheme through NIELIT, CDAC etc.
 - Launching formal courses on virtual mode using the NKN Network to expand the training capacities
- Training of Government Personnel
- Creation of mass information security awareness targeted towards
 - Academic Users: School Children, Parents & Teachers, College level – Students & Faculty
 - General Users: Small enterprises/Business users, SME Sector/Non IT industry, NGOs, CSCs, Cyber cafes and general public at large
 - Government Users: Central/State Government employees (non IT professionals), Legal / Police personnel etc.

Academic Courses

- M.Tech in Information Security
- M.Tech in Comp.Sc. with specialisation in IS
- Retrofitting of B. Tech and M. Tech
- Diploma in Information Security
- Certificate Course in Info. Security
- Short-Term Courses in Info. Security
- Certification Scheme in Information Security by DOEACC Society, Gorakhpur



For further details on Academic Courseware visit :
<https://isea-pmu.in/media/draftSyllabus/FinalSyllabus.pdf>



सी डैक
SDC

BOOTH 04



END-TO-END NEXT GEN SIEM

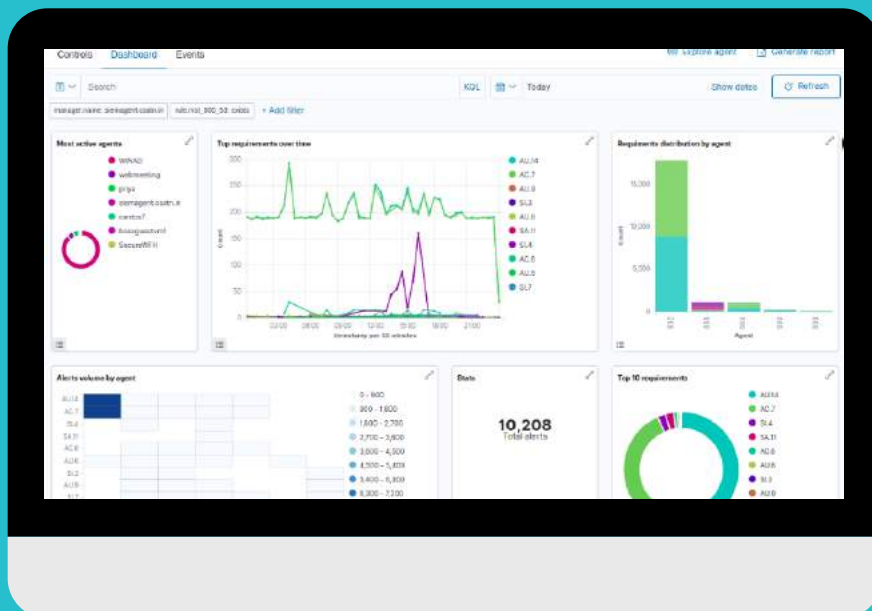
BOSS SIEM



NEXT-GENERATION DETECTION, ANALYTICS & RESPONSE PLATFORM

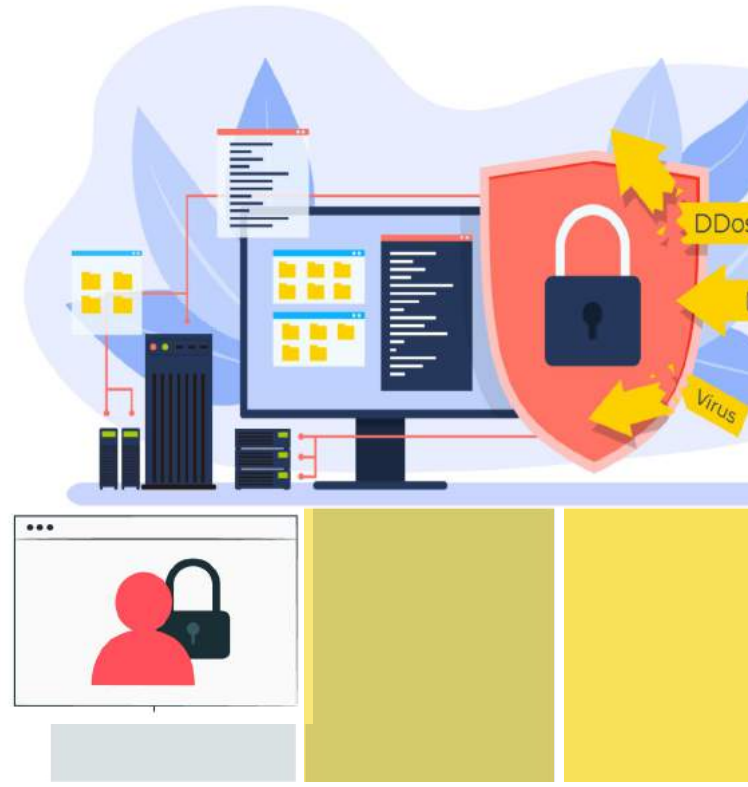
Mail : ethirajand@cdac.in

Call : 9884480819





WE HELP TO ENSURE A RESILIENT CYBER INFRASTRUCTURE FOR THE STATE;



CERT

Computer emergency response team

To serve as a trusted central point within the state to collate information regarding computer security incidents. To issue guidelines, advisories, vulnerability notes relating to information on security practices, procedures, prevention, response and to report cyber incidents.

SOC

Security Operation Centre

To monitor, collect and perform vulnerability analysis on community of network users and service providers. Measures to prevent and handle cyber security incidents.

SAF

Security Architecture Framework

To establish Meghdoot cloud computing platform. To integrate various Enterprise Solution using Central User directory, Enterprise Management solutions, Document Management Solution and to provide other value added service/solution

ABOUT US



Centre for Development of Advanced Computing (C-DAC) is the premier R&D organization of the Ministry of Electronics and Information Technology (MeitY) for carrying out R&D in IT, Electronics and associated areas.

WHY CHOOSE US!

- ☑ In-house development, OpenSource and customized software by CDAC
- ☑ Capability to provide technically suitable domain security experts.
- ☑ Ability to provide Incident Management Service and Vulnerability Assessment Service



info.cet@tn.gov.in
<https://cert.tn.gov.in/>



8th floor, D Block, TIDEL Park,
No. 4, Rajiv Gandhi Salai, Tharamani,
Chennai, Tamil Nadu 600113



044 22542226,
044 22542227

Information Its Lifeline of the Business

As technology advances and access to markets expand, the need to protect information to ensure its confidentiality, integrity and availability has become paramount importance for any organization. Moreover, the strategic and privacy value of the information flowing through the computer networks of any organization makes it very important to see that this information is not stolen, tampered or opened to unauthorized access. The security of the information and the information resources cannot just be entrusted to the technology alone. We need to reach a hybrid solution integrated with human and technology factor into it.

Information Security is one of the most critical concerns facing organisations today. Failing to recognise and manage these risks could seriously jeopardise even the most successful business, leaving it vulnerable to costly interruption of operations – or even more serious security hazards. Safeguarding your organisation is only possible when you fully understand the types and levels of risk your business faces. Our corporate risk assessment will identify all your security issues for you.

C-DAC Information Security Services Consultancy Team comprising of globally recognized certified professionals with rich R & D experience can offer the following:

- ✘ To provide Information Security Consultancy in Secure Data and processing
- ✘ To make Organization understands Information related risks towards them
- ✘ Know the means to reduce risks
- ✘ Mitigate the impact whenever a risk occurs
- ✘ Evaluation of Security Practices of an Organization
- ✘ Identify the risk threats to your organization
- ✘ Develop Policies, Standards, and guidelines suitable to your organization
- ✘ Identify and recommend for suitable Security Practices of an Organization
- ✘ Defining the implementation plan to achieve security goals of an Organization

The need of Information Security Services

Information Security is essential in order to prevent potentially expensive and embarrassing security lapses. There is need of detailed assessments of the Organizations entire security infrastructures to identify and eliminate any vulnerability.

- ✘ Protecting organization's assets like information, devices, services
- ✘ Preventing financial loss through frauds, attacks (Physical or Technical)
- ✘ Preventing losses due to unreliable business systems and processes.
- ✘ Proving due diligence and compliance to your industry regulators, customers and shareholders.
- ✘ Protecting your values by avoiding loss of consumer confidence and business reputation

Standards, Methodologies and Guidelines followed by C-DAC

- ✓ Cert Guidelines
- ✓ Open Web application Security Project (OWASP)
- ✓ ISO/IEC 27002
- ✓ ISO/IEC 27005
- ✓ ISO/IEC 27033
- ✓ PCI -DSS
- ✓ NIST – National Institute of Standards & Technology
- ✓ CIS Benchmarks – Centre for Internet Security
- ✓ OSSTMM – Open source security testing methodology manual
- ✓ Best practices from SANS, ISACA, COBIT etc.,

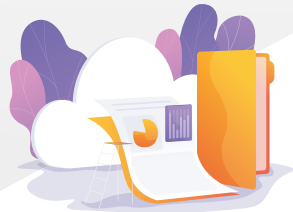
**More than 80 Certified Professionals
in CEH, ECSA, CISP, CISSP, SANS GIAC, ISMS**

C-DAC is Cert-In Empaneled Organization



Meghdoot

Meghdoot Cloud Suite



Free & Opensource suite powered by Openstack
 The only authorised Indian partner of Openstack in training consulting & integration
 Multi-hypervisor support
 Hyper Converged Infrastructure with SDN & SDS

Datacentre Management Suite

Selfservice & Infra Agility
 Auto Discovery of infrastructure both physical & virtual entities
 Automated Scaling with Cloud Orchestration
 Automated Backup & Snapshot Utility



Meghdoot Security Services

Secure VM & Volume Encryption
 Image Signing with Key Managers
 DDOS prevention with Quota Management
 Critical & Non-critical Application Zones Management
 LDAP/AD with RBAC



Meghdoot Cloud Services

Customized Corporate Training
 On-Premise Cloud Solution
 Consultancy Service
 Operation,Management of Cloud



Secure VDI Solution

Deliver an exemplary User Experience
 Deploy Virtualized Desktops across end-user workforce
 Offers Secure Remote access of Intranet Applications from Home`



Centre for Development of Advanced Computing
 8th floor, D South & North Block, TIDEL Park,
 No. 4, Rajiv Gandhi Salai, Tharamani, Chennai, Tamil Nadu 600113

Email : cloud-chn@cdac.in
Phone : 044-2254226/27





सी डैक
CDC

BOOTH 05



AI BASED DIGITAL FORENSICS TOOLSET

Brief Description:

In the domain of Digital Forensics Platform, an R&D initiative has been taken by ICT & S Group of CDAC Kolkata where cutting edge technologies have been applied for automatic analysis of digital evidence for forensics purpose. By applying Natural Language Processing, Image Processing and Advanced Network Analysis techniques, AI based Knowledge Support System known as DIGIFAI Toolset will answer different questions like what a forensics text 'says', who is the author and whether the claimed digitized or handwritten text is genuine or false etc. The DIGIFAI Toolset contains three major components viz. Machine Learning Based Text analytics Tools (DIGITEXT), Image Processing Based Document Forensic Tools (DIGIDOC) & Monitoring of Violence and provoking Activity in Cyber Space (DIGIMONITOR). DIGITEXT can be used as a component of Psychological Autopsy / Equivocal Death Analysis (EDA). Given a Suicide Note the genuineness or credibility of the note can be identified by analyzing various psycholinguistic patterns / emotional tones extracted from the note. DIGIDOC apply image processing and pattern recognition techniques to help forensics experts to examine or verify the authenticity of a questioned hand-written document that could be used as evidence in court or aid in an investigation. DIGIDOC also assist the questioned document examiner to analyze handwritten signatures present in the documents which carry significant information in case of forensics. DIGIMONITOR applies suitable strategies for Real Time Monitoring of the Cyberspace using AI and Network Theoretic tools for investigating criminal activities and help forensic investigators in two ways: a) generating alarm before the actual crime and b) after crime forensics. DIGIMONITOR continuously monitor cyberspace to investigate ongoing tensions like communal riots and agitations that sometime leads to the increase in scale of violence causing immense damage to life and property.

Benefits:

- Investigative Platform for forensic analyst or police investigators
- User-Friendly Interactive Interface; Interactive choice of attributes and prediction algorithm
- AI-enabled system to identify the genuineness of a Suicide Note.
- Automated Writer Verification and Signature Analysis
- Visualization of Writer Specific Attributes for Comparative Analysis
- Similarity Analysis between known and questioned documents of the suspected person

Multistage Attack Prediction using Machine learning

Multistage Attack

Majority of today's breaches are multi-stage attacks. The stages of such attacks can best be described by a Cyber Kill Chain, which breaks down cyber intrusions into

- Reconnaissance
- Vulnerability discovery
- Leverage Exploit
- Delivery
- Malware Delivery
- Malware Execution
- Steal / Sabotage / Destroy/perform C&C.

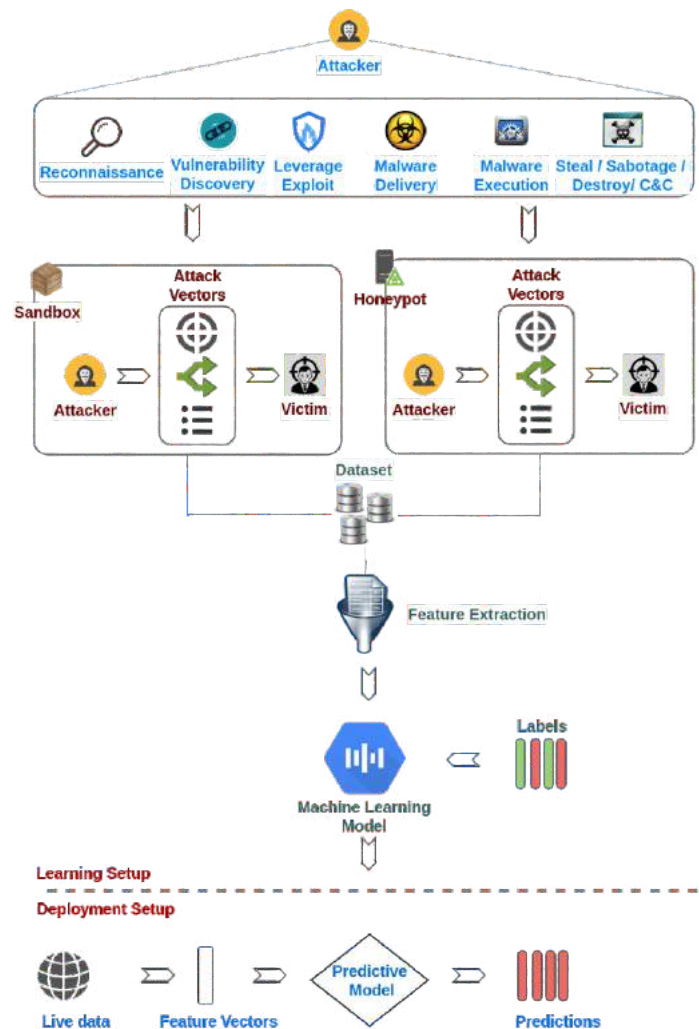
Some of the popular multi-stage attacks include Duqu, Petya, Wanna cry, Locky, Stuxnet, etc.

Our Approach

Our solution leverages ML models to detect multistage attacks. These machine learning models are trained on features and dataset inline with MITRE adversary techniques. This facilitates security experts from seeing the full context of the attack

Salient Features

- Analyze executable programs (PE), DLL
- Static analysis
- Behavioral Analysis
- Network Malware Traffic
- Visualize attack and maps it to the MITRE ATT&CK Framework





BOOTH 06





qkdSim

a QKD simulation kit

Description:

An end-to-end simulation software for performance evaluation of Quantum Key Distribution experiments, that includes realistic experimental imperfections

Abstract:

Just as the 20th century was named the “information age”, the 21st century is often referred to as the “quantum age”, for quantum physics being readily employed to enhance the performance limits of several applications, including metrology, coherent communication and cryptography. Quantum Key Distribution (QKD) is the most mature field of quantum cryptography that enables two parties to securely communicate with each other by establishing a secret key string. While the state-of-the-art classical public-key cryptographic standards (PKCS), such as PKCS #12, are devised on the Rivest-Shamir-Adleman (RSA) algorithm that exploits computational complexity of factoring large numbers for providing security, and hence are not unconditionally secure; the security of QKD is guaranteed by the principles of quantum physics.

With the unprecedented development and commercialization of practical QKD systems, the demand for a QKD simulation software that can include experimental imperfections, and thus can reliably assess the performance of QKD protocol setups before resources are actually invested to implement them, is growing rapidly. We introduce such a cost-effective simulation toolkit “qkdSim”, that offers an end-to-end simulation of QKD protocol implementations using a discrete event-based approach, while considering the experimental nonidealities.

The current version of the toolkit is capable of simulating an experimental demonstration of a prepare and measure based QKD scheme, namely the B92 protocol, and the simulated results show a good agreement with its actual in-lab experimentation. qkdSim overcomes the limitations of the other available QKD simulation software packages by offering realistic modeling of the involved physical processes and components, as well as nearly exhaustive inclusion of practical imperfections.

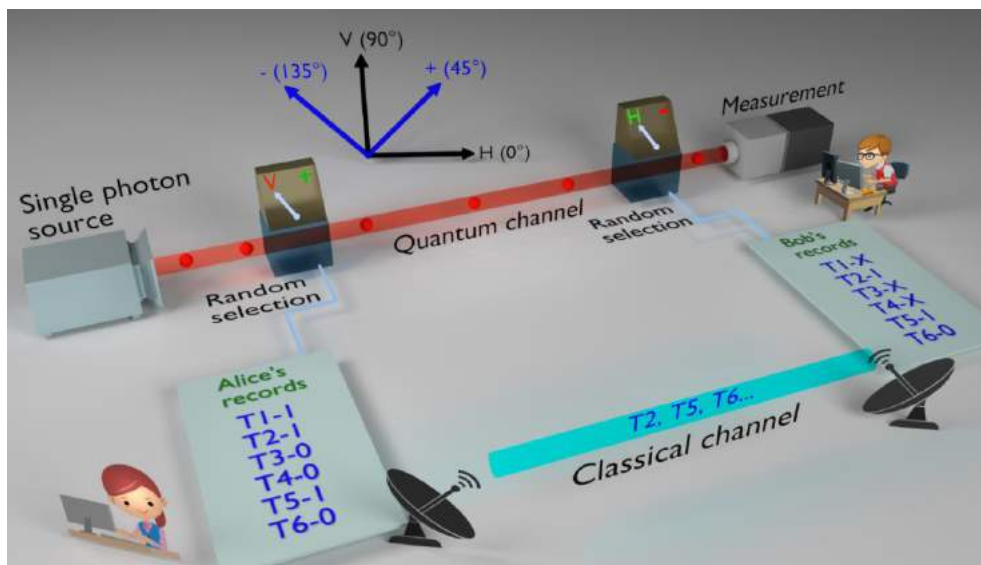
Our toolkit has been built in modular structure that encourages easy accommodation of more features, wider set of imperfections, and the simulation of any generic QKD protocols. More particularly, its “Agifall” architecture allows such a modelling procedure by supporting both sequential and iterative development as per the protocol requirements. The inputs to the simulator consists of the various parameters that are relevant to the experimental implementation of the QKD protocol under consideration. Whereas, the outputs of the simulator are primarily the key rate, the quantum-bit-error-rate (QBER), and



qkdSim

a QKD simulation kit

the key symmetry that evaluate the performance of the protocol implementation. Furthermore, it can be used to analyze the scaling of the key rate and the QBER over a range of one or more input parameters, while keeping the others fixed. This can help in choosing the optimal setting of these parameters required to obtain the best performance from the considered implementation. Finally, qkdSim's data analysis module offers sophisticated optimization strategies to constrain the key rate within the information-theoretically secure bound of QBER, while maintaining a definitive key symmetry. In this way, qkdSim not only provides a comprehensive analysis of a QKD protocol implementation, but also allows to distill a key rate that is information-theoretically secured by the laws of quantum mechanics.



Supporting links:

Link to our article: <https://doi.org/10.1103/PhysRevApplied.14.024036>

Contact Details:

Prof. Urbasi Sinha,

Address : Raman Research Institute, C. V. Raman Avenue, Sadashivanagar,
Bangalore - 560 080, India.

Email : usinha@rri.res.in



BENNETT
UNIVERSITY
TIMES OF INDIA GROUP

BOOTH 07



Abstract

Mobile environments are highly vulnerable to security threats and pose a great challenge for the wireless and mobile networks being used today. Because the mode of a wireless channel is open, these networks do not carry any inherent security and hence are more prone to attacks. Therefore, designing a secure and robust protocol for authentication in a global mobile network is always a challenging. To remedy the security weaknesses in mobility networks, a DNA (Deoxyribose Nucleic Acid) based authentication scheme using Hyper Elliptic Curve Cryptosystem (HECC) has been introduced.

Model

GLobal MObility Network (GLOMONET) provides the global roaming service that permits an authorized Mobile User (MU) to access the services provided by the Home Agent (HA) in a Foreign Network (FN). It is well-known that the wireless and mobility environments are more prone to security threats. An adversary can eavesdrop, modify, or block the sensitive-information communicated through the radio link. Accordingly, the mutual authentication between communication entities in the mobility environment is very essential [1]. This Proposed DNA authentication scheme consists of:

- 1) Registration phase
- 2) Login and authentication phase
- 3) Password change phase

DNA Authentication System

1. The proposed system make use of DNA cryptography to encrypt an MU password based on the DNA sequence.
2. The information enciphered by the DNA sequence is used to authenticate the users.
3. To encrypt the password message using DNA, first map the password (PW) with DNA nucleotides using sequence.
4. The corresponding DNA nucleotides are encrypted using HECC to obtain the cipher text.

Security Analysis

The proposed protocol provides several security services which include, achieves user anonymity and, untraceability, mutual authentication, resistance to insider attack, stolen verifier attack, impersonation attack, replay attack, denial-of-service attack and provides Forward secrecy and secure key establishment [2]. We used the Automated Validation of Internet Security Protocols and Applications (AVISPA) to analyse the security of the proposed protocol. The AVISPA tool is widely used to examine the correctness of the formal security properties of authentication schemes. In AVIPSA, the authentication protocol is implemented in High Level Protocol Specification Language (HLPSSL). The code implemented in HLPSSL is translated into intermediate format (IF) using HLPSSL2IF translator. This IF is fed into one of the AVISPA back-ends to produce the output format (OF). Finally, AVISPA uses OF in order to verify whether the given authentication protocol is safe or unsafe against active and passive attacks in the networked environment [3].

Results

Assume that the authentication protocol using ProVerif has parallel processing capability among communication agents like MU, FA, and HA. These agents can generate, send and receive information from each other, and verifies the received information. The attacker A in the formal model is able to hear, intercept, retransmit or modify the messages. By using pi calculus we have modelled the proposed protocol, then it is interpreted into Horn clauses. Generally, ProVerif output is a confirmation of the security requirement that satisfied is true or false. The goal role specifies the security requirements which the proposed authentication protocol requires to meet. The proposed mutual authentication protocol is simulated through AVISPA web tool under the ATSE (ATTC Searcher) and OFMC backends. The AVISPA result comprises of the following segments:

1. SUMMARY: Which specifies that whether tested authentication protocols are safe or unsafe.
2. DETAILS: Describes under what criteria the tested protocols are concluded as safe or unsafe.
3. PROTOCOL, GOAL, and BACKEND: This section denotes a protocol name, goal of the protocol analysis and name of the backend used in AVISPA tool.

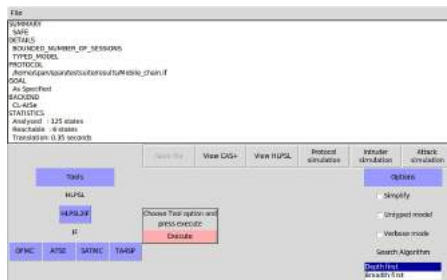


Fig. 1: Result analysis.

The AVISPA result analysis through OFMC as a backend is shown in Fig. 1. It is evident from the results that the proposed authentication protocol is safe and satisfies the design goals for roaming service in mobility environments. Further, the proposed protocol is verified using security protocol animator (SPAN) tool to detect and build a message sequence chart (MSC) to represent the possible attacks and intruder activities. In this manner, we have proved that our proposed protocol is faithful, and the legal participants MU, FA, and HA can authenticate each other. Moreover, the proposed authentication protocol establishes a secure session key. The proposed authentication protocol and some other recent protocols in terms of functionalities, computational and communication cost. The proposed protocol is analyzed and differentiated with recently introduced protocols for authenticity in global mobile networks

Performance Comparison

In order to evaluate the computational performance of the proposed authentication protocol in resource-limited devices, several cryptographic operations have been simulated using a Crypto library on a smartphone. The smartphone runs on the Android operating system of an Arm Cortex-A8 processor with the frequency of 0.72 GHz. The cryptographic operations are implemented in C++ language under Crypto++ library (MIRACL) [39]. Further, the hash operation, symmetric and asymmetric encryption/ decryption operations are implemented by the secure hash algorithm (SHA-160), advanced encryption standard with cipher block chaining (AES-CBC) and the elliptic curve-integrated encryption scheme (ECIES), respectively

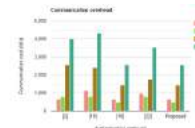


Fig. 2: Comparison of Communication cost.

Conclusion

The primary merit of the proposed protocol is simplicity, resistance against various attacks, and practicality for implementation under expensive and insecure wireless network environments. One of the future research direction includes extending the proposed DNA based password authentication system to IoT (Internet of Things) environment, in order to ensure secure communication between users and IoT devices.

Acknowledgements

I would like to thank Data Security Council of India (DSCI) for funding grant to accomplish the project successfully and I am very grateful to all my colleagues of Bennett University for their assistance.

References

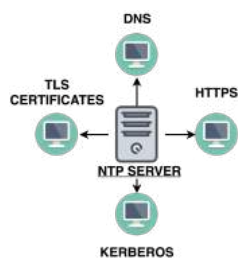
- [1] Shashidhara R and R Madhusudhan. "A Novel DNA Based Authentication Protocol for Roaming Service in resource-constrained Environments". In: *Multimedia Applications and Tools 45* (Mar. 2020), pp. 55–66.
- [2] Shashidhara R and R Madhusudhan. "A Secure Anonymous Authentication Protocol for Roaming Service in Resource-Constrained Mobility Environments". In: *Peer-to-peer Networking and Applications 12* (Apr. 2020), pp. 153–194.
- [3] J. Watanabe. *Group Theory*. Singapore Mathematical Society, 2010, p. 75.

NETWORK TIME PROTOCOL VULNERABILITIES ASSESSMENT AND DEFENSE MECHANISM

INTRODUCTION

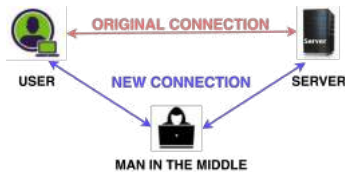
- NTP is used to synchronize time between computer systems and the internet.
- Vulnerability assessment of NTP based attacks.
- Building defense mechanism.

APPLICATIONS OF NTP



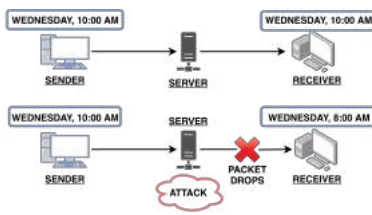
Man in the Middle Attack

- Attacker is in a conversation between two parties, gains access to information that the two parties were trying to send to each other.



Time Shift Attack

- The time shift between a client's clock and a server's clock.

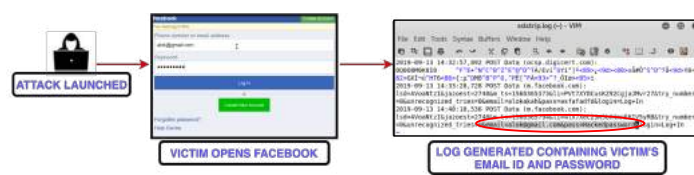


TOOLS USED

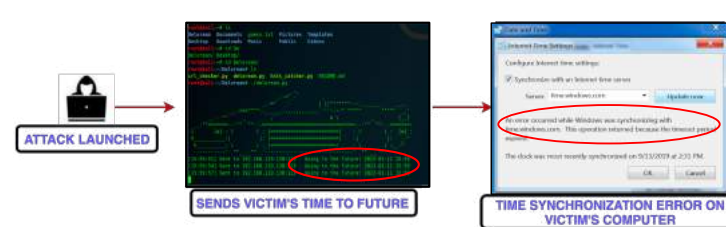
- WINDOWS OS
- KALI LINUX
- ETTERCAP
- PYTHON IDE

RESULTS

Man in the Middle Attack



Time Shift Attack



CONCLUSION

- This Project lays emphasis on various NTP based vulnerabilities or loopholes.

DEFENSE

- Our aim is to design a defense mechanism to capture such packets and drop them.

NTP REFLECTION ATTACK



REFERENCES

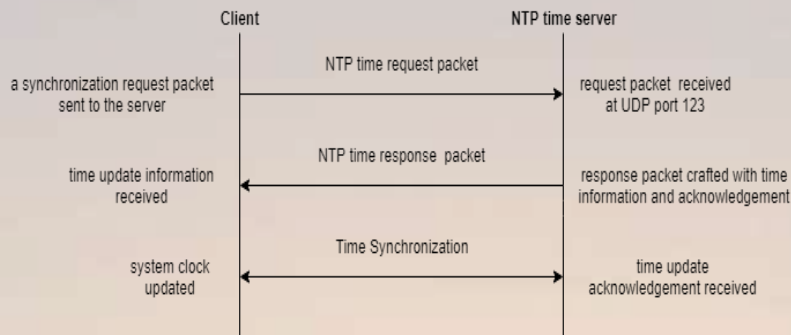
- Malhotra, Aanchal, and Sharon Goldberg. "Attacking NTP's Authenticated Broadcast Mode." *ACM SIGCOMM Computer Communication Review*, vol. 46, no. 1, 2016, pp. 12–17, doi:10.1145/2935634.2935637.

AUTHOR: ALOK KUMAR MISHRA
MENTOR: MAYANK SWARNKAR

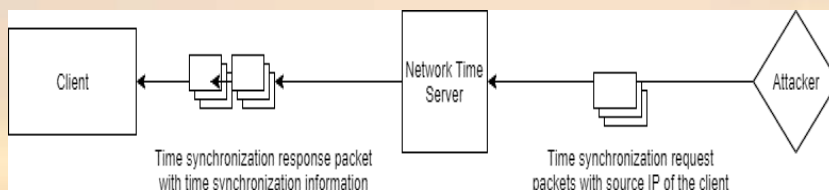
Vulnerability Analysis On Network Time Protocol

The project aims at testing protocol's ability for handling high frequency flow of data packets by means of Denial of Service, Reflection and amplification attacks using GET monlist packets

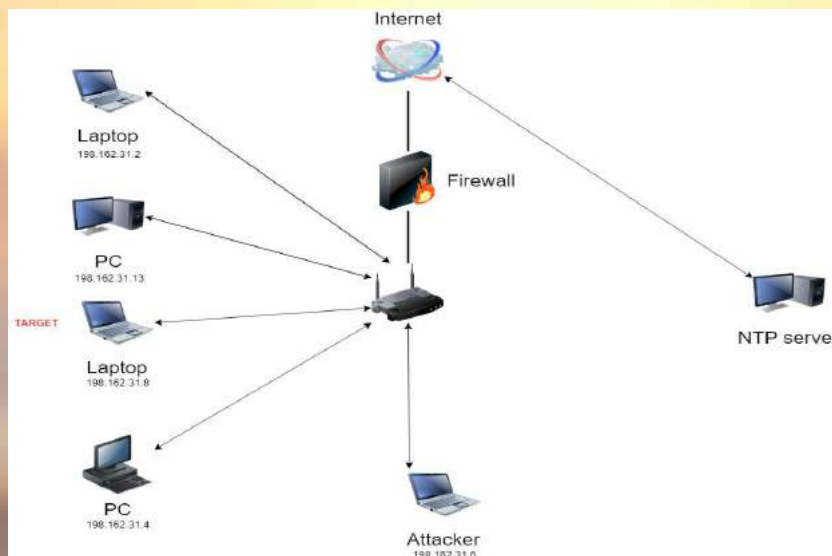
Working Of NTP:



Reflection and Amplification attack:



Experimental Setup:



Results:

- A successful DoS attack on a NTP client using reflection and amplification attack.
- Analysis of the attack done in respective with the NTP client, checking three main parameters : Bandwidth, CPU speed, and Memory
- A proposal for detection method using frequency analysis of received and sent NTP monlist request and response messages



SUYASH ANAND TRIVEDI
E16CSE135



Mentored by-
Dr. MAYANK SWARNKAR

Violent Action Recognition using Drone Surveillance

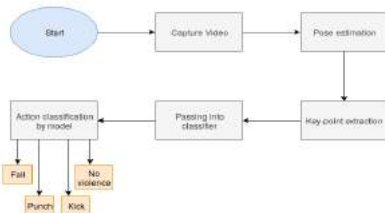
Divyaansh Devarriya, Anosh Billimoria



Abstract

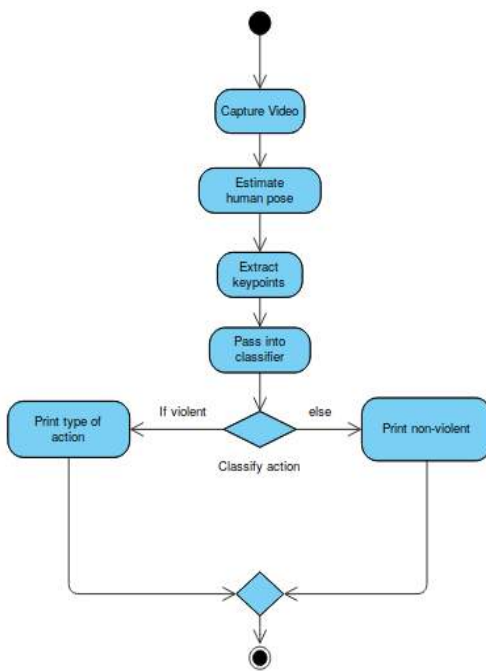
- Although action recognition is a widely studied field in computer vision, the recognition of aggressive activities and crowd's violent actions are comparatively less studied.
- Our work introduces a model for drone surveillance system to identify violent activities in public areas.
- The system first uses a neural network for human pose estimation[1][2].
- The system then performs keypoints extraction from the estimated pose.
- The keypoints of the estimated pose are then used to recognize the violent activities.

Introduction



Proposed Method

Activity Diagram of the method



Pose Estimation

- A skeleton is formed by joining 18 key-points for each human in the frame is detected using part affinity fields [2].
- Confidence values for the key-points is also calculated.

Keypoints Extraction

- Key-points of the estimated human pose are extracted for each human.
- The extracted key-points are written in a csv file along with number of keypoints detected, average confidence of the key-points and person label.

Action Classification

- In the last phase, the key-points extracted are converted into a vector or an array.
- The vector is labelled for each action.
- The set of labelled vectors are then used for multi-class classification.

Experimental Results and Discussion

- We proposed an annotated violent activities dataset taken from drone camera to be used by the key point detection network to learn pose estimation.
- The dataset has around 15-20 videos for each violent action.
- The dataset includes four violent activities (1) Punching (2) Kicking (3) Falling (4) Non-violent actions



Data collected using Drone



Pose estimation on the data

Type of data	Accuracy
Training	100%
Testing	91.66%

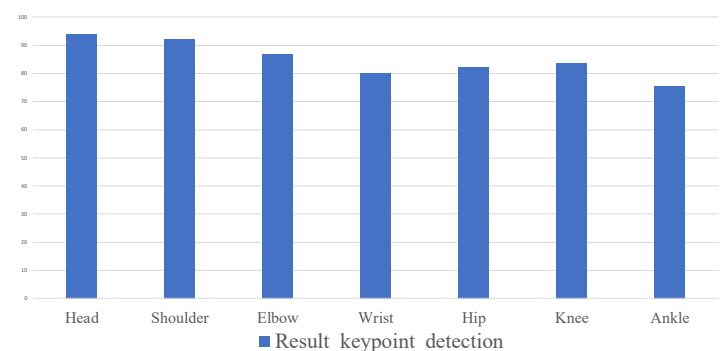
Accuracy of train and test data

Class	Accuracy
Punch	100%
Kick	100%
Fall	85.71%
Non-Violent	66.66%

Accuracy of each class

664	241	623	312	663	316
788	222	840	276	818	272
663	243	621	312	661	316
787	224	839	277	818	272
661	243	620	312	659	316

Sample key-points data



Conclusions

- This work proposed a Drone Surveillance framework that can detect one or more individuals engaged in violent activities from aerial images.
- The runtime performance of this framework is computed based on (i) human pose estimation using part affinity fields (ii) key-points extraction (iii) classification of the actions based on extracted key-points.
- The performance of action classification detection model is affected by the number of humans in the aerial image. It is easier to train and evaluate model's performance if there's a single person in the video.

References

- https://github.com/michalfaber/keras_Realtime_Multi-Person_Pose_Estimation
- Cao, Z., Simon, T., Wei, S.E. and Sheikh, Y., 2017. Realtime multi-person 2d pose estimation using part affinity fields. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 7291-7299).
- Singh, A., Patil, D. and Omkar, S.N., 2018. Eye in the Sky: Real-time Drone Surveillance System (DSS) for Violent Individuals Identification using ScatterNet Hybrid Deep Learning Network. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops* (pp. 1629-1637).
- Shuai, S., Kavitha, M., Miyao, J. and Kurita, T., Action Classification Based on 2D Coordinates Obtained by Real-time Pose Estimation.

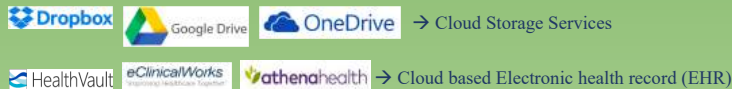
On Solving Data Possession Issues in Cloud based Electronic Health Record System

Sanjeet Kumar Nayak

Assistant Professor, Department of CSE, Bennett University, Greater Noida, India-201310

Email: sanjeet.nayak@bennett.edu.in

INTRODUCTION

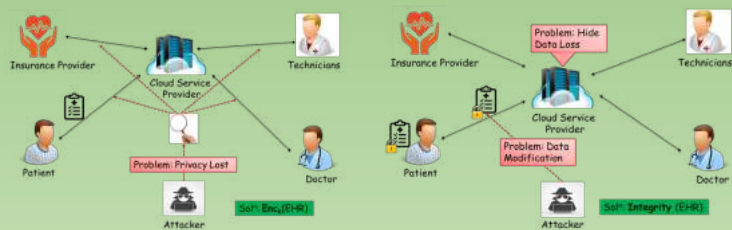


Major benefits of EHR

1. Up-to-date and complete information
2. Less medical errors
3. Reliable prescription

Major benefits of cloud based EHR

1. Low initial infrastructure setup
2. Relief from maintenance overhead
3. Universal access to the data



How to efficiently verify the correctness of outsourced data?

- Simply downloading the EHR data and verifying is not practical

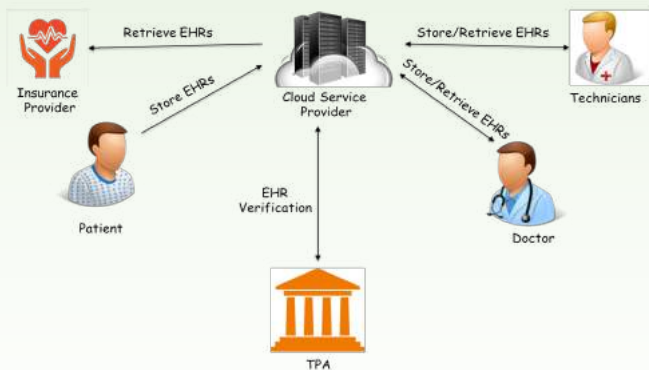
LITERATURE REVIEW

Schemes	Blockless Verification	Public Auditability	Privacy Preserving	Data Dynamics	Batch Auditing	Lightweight Verification
Shacham et al. Scheme - 1 [2]	Yes	No	No	No	No	No
Shacham et al. Scheme - 2 [2]	Yes	Yes	No	No	No	No
Wang et al. Scheme [4]	Yes	Yes	Yes	No	Yes	No
Zhu et al. Scheme [3]	Yes	Yes	Yes	Yes	No	No
Wang et al. Scheme [4]	Yes	Yes	Yes	Yes	Yes	No
Yang et al. Scheme [5]	Yes	Yes	Yes	Yes	Yes	No

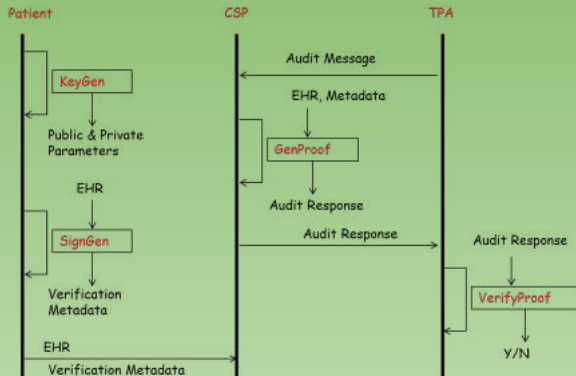
MOTIVATION

- Verification consist of time consuming pairing operations
- Not suitable for performing verification in mobile devices
- Can we verify without pairing operation? (Lightweight Verification)

SYSTEM MODEL

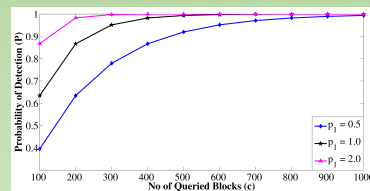


PROPOSED SCHEME – OVERVIEW



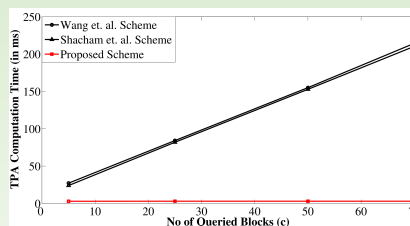
SECURITY ANALYSIS

- Storage Correctness
- Blockless Verification
- Unforgeability
- Privacy Preserving
- Misbehavior detection



COMPUTATION COST COMPARISON

Schemes	Overall Computation Cost
Shacham et al. Scheme [2]	$2T_p + (2n+2c+2)T_c + (n+3c-1)T_m + (n+c)T_h$
Zhu et al. Scheme [3]	$4T_p + (2n+2c+6)T_c + (2n+4c-1)T_m + (n+c+2)T_h$
Wang et al. Scheme [4]	$2T_p + (2n+2c+5)T_c + (n+3c+1)T_m + (n+c+2)T_h$
Yang et al. Scheme [5]	$3T_p + (n+2c+6)T_c + 2cT_m + (n+c)T_h$
Proposed Scheme	$5T_c + (2n+3c+1)T_m + (n+c)T_h + T_i$



CONCLUSION & FUTURE WORK

- A privacy preserving provable data possession scheme for cloud storage based EHR is presented.
- The proposed scheme provides lower computation overhead for the TPA as compared to the other existing schemes.
- Applications
 - Audit network log
 - financial banking data
- Future Work
 - Extend the proposed scheme, where multiple stakeholder of the cloud based EHR are present considering access control for each one of them.
 - Further, we also need to study the behaviour of batch auditing and data dynamics requirement

SELECTED REFERENCES

[1] S. K. Nayak and S. Tripathy, "SEPPDP: Secure and Efficient Privacy Preserving Provable Data Possession in Cloud Storage," IEEE Transactions on Services Computing, 2018.

[2] H. Shacham and B. Waters, "Compact proofs of retrievability," In Proc. of 14th ASIACRYPT, Pages: 90-107, 2008.

[3] Y. Zhu, H. Hu, G. J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," IEEE Transactions on Parallel and Distributed Systems, 23(12), Pages: 2231-2244, 2012.

[4] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Transactions on Computers, 62(2), Pages: 362-375, 2013.

[5] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Transactions on Parallel and Distributed Systems, 24(9), Pages: 1717-1726, 2013.

[6] L. Guo, C. Zhang, J. Sun, and Y. Fang, "A privacy-preserving attribute-based authentication system for mobile health networks," IEEE Transactions on Mobile Computing, 13(9), Pages: 1927-1941, 2014.

Introduction

Our project helps detect malicious executable using a smart executable analyzer. Operating systems users like of Microsoft Windows often have to manually download files from online websites instead of a central trusted repository and may end up downloading malicious executables that are frequently disguised as Screensavers or images. These file extensions go undetected by the layman and sometimes even a professional.

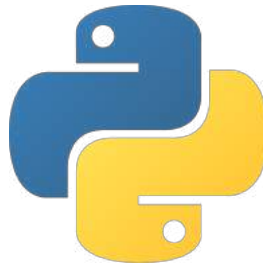
Problem

Most malware detection softwares need to be regularly updated to be able to keep up with the rapidly rising threats in the cyber world. Sometimes even this doesn't help.

Solution

Using Machine Learning to be able to identify malicious files that are new and would go undetected otherwise. Training our model to accurately identify malicious executables and hence reducing the false positive rate.

Techniques Utilized



.We used Python predominantly to create our model and train it, as well as to examine the dataset procured. We used Jupyter Lab to execute our code.

Demo Snapshots

```
File Number(Malware): 7
Desktop\files\r.dll

File Number(Malware): 8
Desktop\files\twain_32rm.dll

File Number(Malware): 9
Desktop\files\WordpadFilter.dll

Total Number Of Files Embedded Icon(Malware): 9
```

Fig. 2. Malicious Files detected

```
Number Of Files: 1
Number Of Files: 2
Number Of Files: 3
Number Of Files: 4
Number Of Files: 5
Number Of Files: 6
Number Of Files: 7
Number Of Files: 8
Number Of Files: 9
Malware Find 0
The time for running this program: 0.061956167221069336
```

Fig. 3. Time taken to scan 9 files

Conclusion

We evaluated this approach on the dataset we were about to procure. The result of our experiments show that the PE-Header-Based approach achieves more than 99% detection rate with less than 0.2% false positive for distinguishing between benign and malicious executables in less than 20 minutes.

Future Work

Creating a user friendly interface, as well as integrating different features to encompass different malware defence systems.



4_Crime_Sinawal-Meb... rplg.zip APT BADINFECT



CVE Equation_KasperskyRep... ples.zip f2a07e3ad5846753023fa.. 32a5.7z



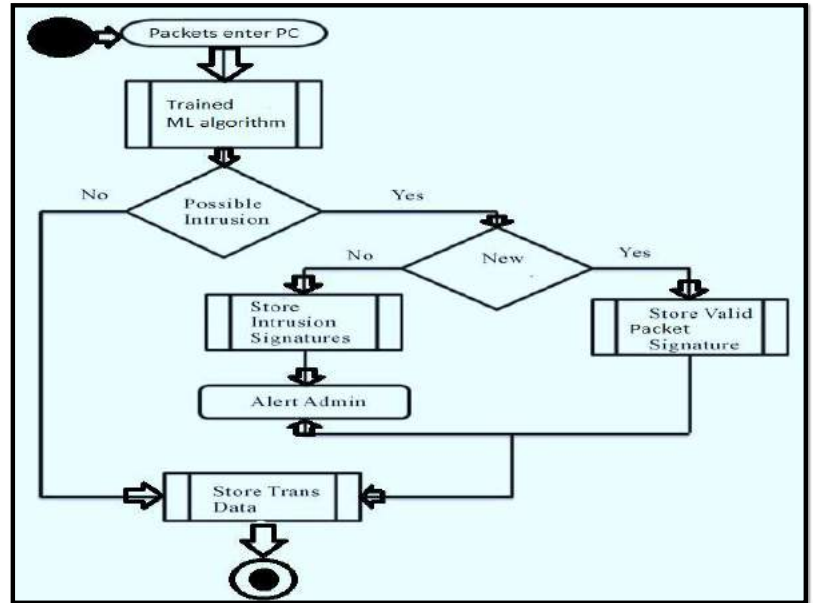
Fig. 1. Dataset

INTRODUCTION

The project aims at making an Intrusion Detection System based on Machine learning approach, to detect intrusions. It uses an anomaly and hybrid based approach which would detect even the newest signatures. Different machine learning models (Naïve Bayes, Decision Tree, Adaboost, Random forest, KNN, Support Vector Machine in linear kernel and then in rbf kernel) were tried in this project. DNNs gave the best accuracies and results.



SCHMATIC PROJECT OUTLINE



APPLICATION

Intrusion Detection System is in high demand, as every person and organization would require a high accuracy and precision system, that would detect and alert the user and protect their private, legal or financial data, from intruders trying to breach in to the computer systems or networks.

“Design of A Secure Privacy-preserving Digital Voting System Using Blockchain Technology”

Krishna Veer Singh
Computer Science Engineering
Bennett University Greater Noida

Abstract

Blockchain is an emerging technology, which offering numerous opportunities to develop decentralised and distributed digital services by ensuring privacy and transparency. The aspect of privacy, authenticity, transparency and security is a threat and challenging in the traditional voting systems. Controversial E-Voting could have been avoided if the election and counting process is transparent, verifiable and secure. The existing voting system does offer anonymity to the voter but the counting process by the officials is not transparent. The voters are supposed to trust the result which is provided by the government body or Election Commission. There are also other electoral flaws like ballot stuffing, voter fraud and booth capturing.

Objectives

- To Design a secure and decentralized Blockchain based E-Voting system using smart contracts (Chain code).
- To propose a user credential model to ensure authentication, authorization and non repudiation services.
- To help the user to cast a vote using private key, following which the transaction will be recorded in the decentralized Blockchain network.

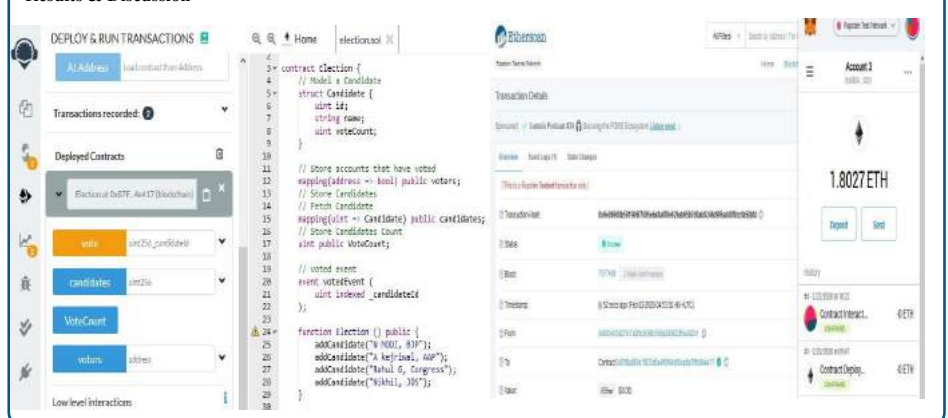
Introduction

Voting is the foundation of any successful democracy and must therefore be accessible and secure for all eligible citizens in the country. Several Electoral systems take on to permit citizens to cast their precious vote, which includes electronic methods, ballot based voting and Electronic Voting Machine (EVM). Existing techniques for voting, based on electronic voting machines, provides mistrust kind of transparency to voters. The issue commonly known as voter confidence. The Voting Systems have to heighten privacy and secrecy to provide electoral services available to the voters but secured against security vulnerabilities like keeping the voter ballot from being modified with the impact of changing casted votes by the voter.

Literature Gaps

The existing voting system does not offer voter privacy and even the vote counting by the officials is also not transparent. The voters are supposed to trust the result which is provided by the government body or Election Commission. Current E-Voting protocols require a centralized authority to monitor and control the whole procedure from ballot to results. The centralised systems are vulnerable to security attacks like DDOS.

Results & Discussion



Methodology

The proposed protocol consists of the following phases:
Setup: This is an initialization phase to obtain the private key and public key pair using asymmetric cryptosystem.
Voter Authentication: The user should logs to the system using the credentials. The protocol will authenticate the voter based on his/her identity information issued by the Election Commission. The E-voting system should verify and validate all information entered by the voter. If the verification is successful, the voter will be authenticated and authorized to cast the vote.
Casting a vote: Voters should choose the candidates from list of contestants to cast their vote. The voter can cast the vote through a friendly user interface.
Formation of the Block: Upon casting the vote by the voter will be recorded as a unconfirmed transaction in the Blockchain. The nodes in the Blockchain network will validate the casted vote based on consensus protocols.
Sealing of Blocks: The transactions are stored in the Blockchain, by the end of polling time all blocks in the network needs to be sealed by cryptographic hash (SHA-256) using nonce and merkle root. Once the electoral process is complete and the results have been published, then there is no significance for the Blockchain mining.

Conclusion

A Blockchain based decentralized and peer-to-peer electronic voting protocol is proposed. The transaction will be recorded in the Blockchain network, which is anonymous and adversaries are unable to modify the records in the network. In order to provide the privacy and transparency of E-Voting protocol, secure cryptographic functions has been employed to ensure that the registration and voting is anonymous. The digital signatures Using public key infrastructure makes the voting process more secure and reliable.

Future Work

For the future work, system can be applied for use case and measurements can be taken to compare if the calculation hold. Synchronization and consensus algorithms can be discussed and improved for better performance and security.

Acknowledgment

I would like to express my sincere gratitude to my guide, **Dr Shashidhar R.**, and I am highly obliged to thank all the staff of the Department of Computer Science Engineering for their continuous assistance.

Decentralized Application (DAPP) for KYC Using



BENNETT
UNIVERSITY
TIMES OF INDIA GROUP

Tushar Inani
(Intern) *Blockchain*

Shashidhar M'lore
(Supervisor)



Abstract

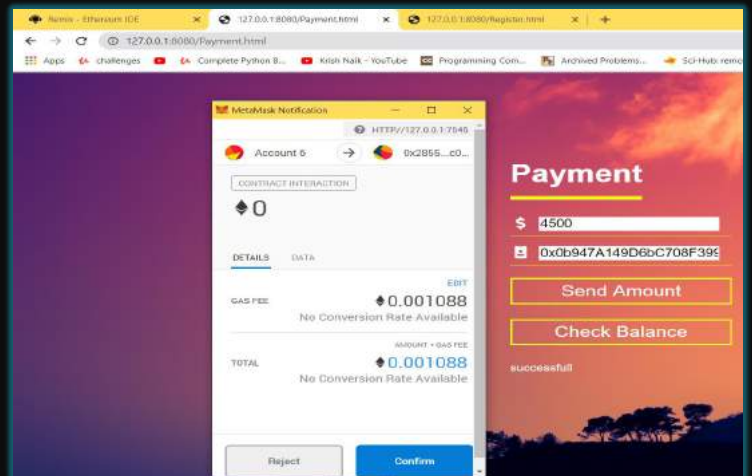
DAPP(Decentralized application) is web application developed in Solidity & Javascript and it is implemented by using Metamask and windows appliance . This application provides an easy and simple way to know the customer (KYC) online. Customers can register themselves and can do money transfer from their accounts. Customers can view their details and wallet balance.

Techniques Utilized



Payment Dashboard

MONEY TRANSFER FROM ONE ACCOUNT TO ANOTHER (DIRECTLY)



Introduction

Know Your Customer (KYC) checks are currently an extremely time consuming and costly affair. Banks have to spend millions of dollars every year to keep up with KYC regulations or risk being fined heavily. Through DAPP, we aim to simplify this process to a great extent.



Conclusion

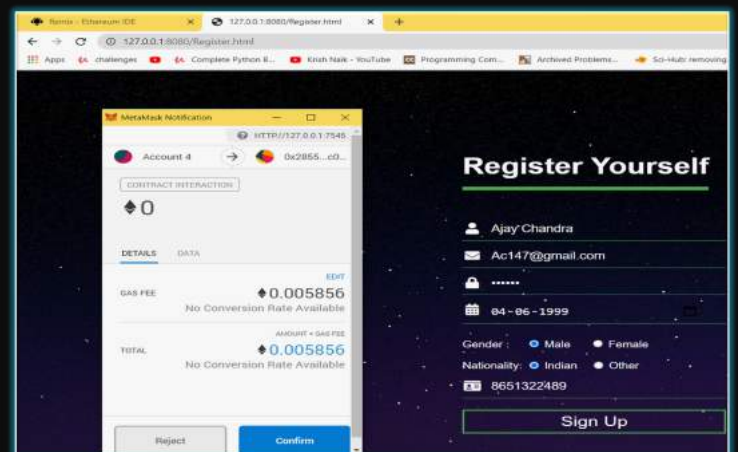
- Registration Details will be stored in Blockchain
- Money can be transferred and the transactions are recorded in Blockchain
- Users can login and check the balance in their respective Accounts

Proposed Method

The Idea is to keep identify information on the **Blockchain** and **Organizations** would verify the identity information of the user through Decentralized app. Here, users can share the required information to the companies. They will verify it using **DAPP**. Also to minimize the fraud and identify theft. In order to achieve transparency, the details should be stored on Blockchain

Future Work

- ❖ Launch it Online
- ❖ Updation in Account Details
- ❖ Make it portable and platform Independent
- ❖ Making the details public for organization





BOOTH 08





Indian Institute of Technology

(Indian School of Mines) Dhanbad

Title:

AI/ML driven Intrusion Detection Framework for IoT Infrastructure

Abstract:

Monitoring systems are responsible for controlling the technology used by a company. Internet of Things (IoT) has emerged as one of the enabling technologies for monitoring systems. It is continuously captured, processed, and transmitted by systems generally interconnected by the Internet and distributed solutions. In today's scenario, IoT driven solutions are available for efficient monitoring systems. However, these infrastructures are vulnerable to various cyber-attacks.

The intruders may intentionally manipulate the data during transmission or disturb the normal functioning of monitoring systems etc. through attacks. That results in the economy and produce loss. We can develop supervised and unsupervised intrusion detection systems. It is started with feature extraction and capture activities of the nodes. The machine learning technique analyzes activities and detect malicious behaviors. Then, the system prevents malicious nodes.

An unsupervised intrusion detection system works for an unlabeled dataset that is free from labeling costs or efforts. Moreover, the micro-clustering method detects unknown attacks or those contain few samples. Hence advancements should be sought on intrusion detection techniques, and considering the same in current research, it is planned to design AI/ML driven framework to address the IoT framework requirement efficiently.

Application Scenario:

Precision farming, power grid system, Body area network, Smart city, Digital twin

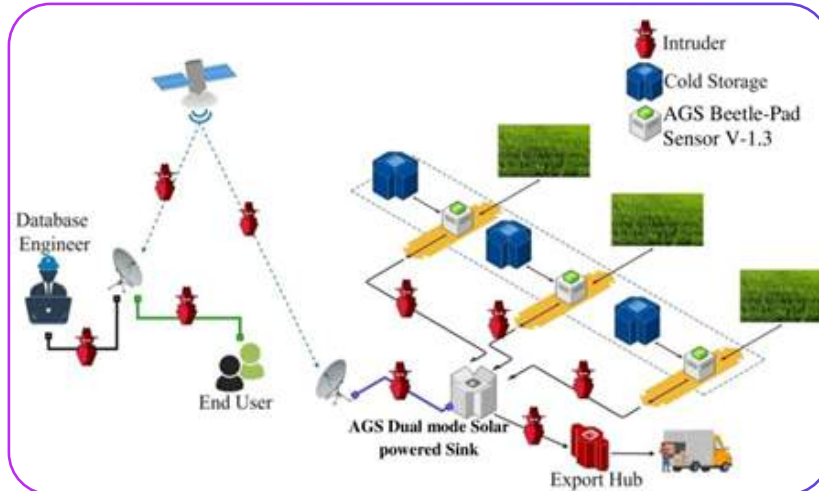
Case Study:

AI/ML driven Intrusion Detection Framework for IoT enabled Cold Storage Monitoring



Indian Institute of Technology

(Indian School of Mines) Dhanbad



- Modeling and deployment of a real-time IoT enabled WSN Infrastructure for Cold storage monitoring and management
- Network traffic analysis for identification of possible Vulnerability point in the cold storage infrastructure accessible to intruder, to prepared training data for intrusion detection framework development.
- Implementation of AI/ML driven training models for intrusion detection
- Testing the performance of developed model by injecting various attacks in network traffic

Supporting link and references:

- Prasad, Mahendra, Sachin Tripathi, and KeshavDahal. "Unsupervised feature selection and cluster center initialization based arbitrary shaped clusters for intrusion detection." Computers & Security (2020): 102062
- Prasad, Mahendra, Sachin Tripathi, and KeshavDahal. "An efficient feature selection based Bayesian and Rough set approach for intrusion detection." Applied Soft Computing 87(2020): 105980.

Contact Details:

Prof. Sachin Tripathi (Associate professor/ Head of Department)
Department of Computer science and engineering, Indian Institute of Technology
(IIT-ISM) Dhanbad

Email : sachin2781@iitism.ac.in



INTERNATIONAL INSTITUTE OF
INFORMATION TECHNOLOGY
HYDERABAD

BOOTH 09





Security Information and Retrieval Extraction eNgine

With increasing internet access and IT dependency, security vulnerabilities, threats and incidents increased manifold. As per some reports, an average of 100,000 websites are hacked every day. Professional hackers, terrorist organizations and in some cases, nations are involved in cyber attacks in the form of social engineering, denial of service, SQL injection, etc.

Users refer to security specific websites or generic search engines for 'information security' related information. However, the content on these websites is not available as actionable information, the authenticity of the information is sometimes questionable and information dissemination is delayed. Availability of prevalent domain specific - 'Information Security Search Engine' improves the awareness and ease the keyword search in security domain.

We demonstrate SIREN (Security Information and Retrieval Extraction eNgine) that extracts publicly available information security text extending Artificial Bee Colony algorithm-based crawlers with computational and network optimization. The extracted unstructured text is enriched into an ontology using state-of-the-art Bidirectional LSTM and Universal Sentence Encoder models for reasoning on vulnerabilities, threats, attacks and many other use cases of SIREN. A FACT score is calculated on the fine-grained surface, content and off web page features to display credible sources of the extracted information.


The URL of SIREN is <https://serc.iiit.ac.in/Bhompoo/infosec.html>



Security Information and Retrieval Extraction eNgine

About Login

SIREN (Security Information Retrieval and Extraction eNgine)



HTTP properties

About 15226 results (0.031 seconds)

[CVE - CVE-2012-1875](#)
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1875>

[LoyaltyPlus Program | RSA Conference](#)
<https://www.rsaconference.com/about/loyaltyplus>

[Webhoneypot: Filter Reports - SANS Internet Storm Center](#)
This page allows you to search our reports for matches to particular header properties... Top of page Contact Us Contact Us About Us Handlers Diary Podcas
News Tools DShield Sensor 404Project InfoSec...
<https://isc.sans.edu/webhoneypot/filter.html>

[Alphabet Announces First Quarter 2017 Results - Investor Relations - Alphabet](#)
2017 Google properties revenues ... properties revenues 3... properties revenues 70 ... of Google properties revenues 8 ...
https://abc.xyz/investor/news/earnings/2017/Q1_alphabet_earnings/
last modified : Thu, 27 Apr 2017 21:02:32 GMT

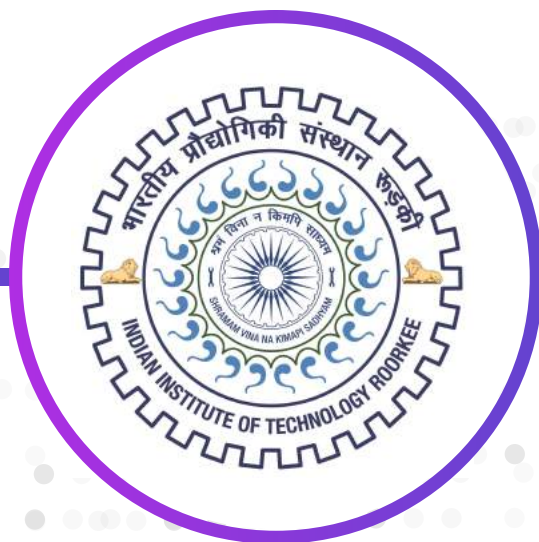
[NIC's Government Partnerships In The News | NIC](#)
<http://www.egov.com/news/news-articles!/content/page/5>

Contact Details:

Lalit Mohan Sanagavarapu, Dr. Y Raghu Reddy

Email : lalit.mohan@research.iiit.ac.in , Raghu.reddy@iiit.ac.in

Web : <https://serc.iiit.ac.in>



BOOTH 10





Reliable data auditing with optimal data encoding parameters
in cloud environment

Executive Summary

To maximize users trust and minimize data losses in the cloud environment, we introduce a reliable data verification mechanism that guarantees correctness of data even during server failure or unavailability of data. First, we investigate optimal encoding parameters that meet the users' expectations to provide higher reliability with a minimal storage cost. To protect the data from the losses, we create multiple coded data and parity fragments. Then we distribute them to the distinct storage servers. Further, we simplify the verification procedure without needing the data aggregation, just by storing the evidence fragments and data fragments across distinct datacenters. Our solution audit the stored data validity over distributed encoded fragments without downloading the stored data fragments to the client system every time. We utilize and leverage the Erasure Coding to propose a reliable storage correctness verification solution that guarantees the retrieval of evidence and minimizes the effect of server failure/unavailability.

Design Goals

Aim is to design an efficient data verification mechanism to achieve the following goals:

- Storage Correctness Assurance: The recommended approach aims to ensure the correctness of dispersed secure encoded fragments across the cloud datacenters.
Selection of Optimal Encoding Parameters: Storage service providers should choose an appropriate encoding scheme with optimal encoding parameters' values. These parameters play a crucial role in providing higher reliability and lower storage costs.
Error Correction and Fault Tolerance: The proposed framework achieves data and signature availability and reliability. It refers to the scenario where the verification process should be unaffected even if some servers are down.
Lightweight Communication: The verification process should exchange small evidence messages rather than actual data between entities.

Methodology

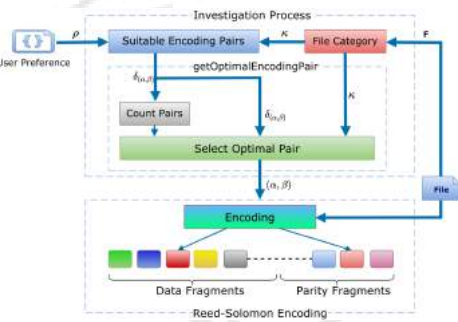


Fig1: Investigation of an Optimal Encoding: It demonstrates the procedure to validate the stored data fragments across the datacenters. To audit the stored data integrity, the user sends the audit request to the TPA and gets back its validity status. Moreover, TPA periodically performs a validity check to ensure the correctness of the stored data.

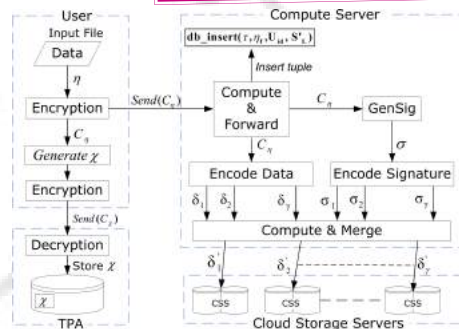


Fig2: Data Uploading Scenario: It demonstrates the proposed upload and dispersal procedure in order to validate stored encoded fragments during the verification phase.

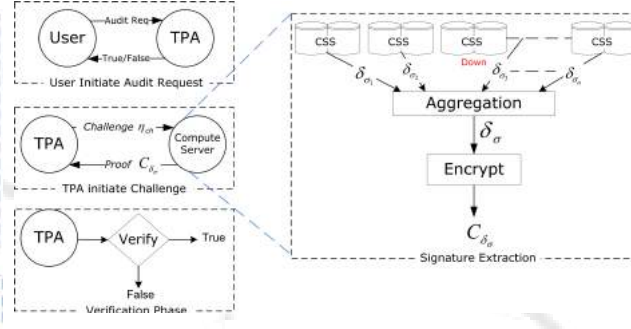
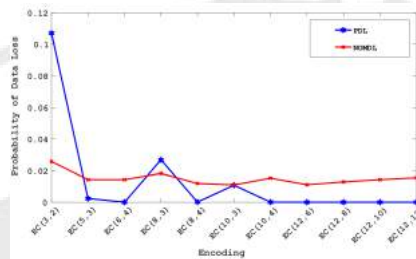
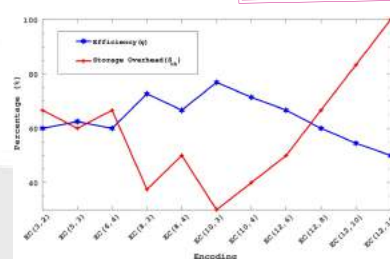


Fig3: Verification Procedure of Coded Fragments: Investigation of optimal data encoding parameters based on user preferences and generation of coded fragments in order to maximize the service performance and availability, minimize the impact of service failures, and enhance the business continuity.

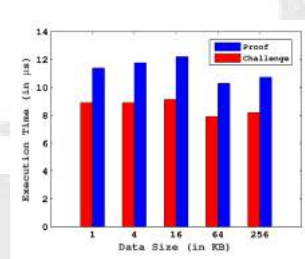
Results



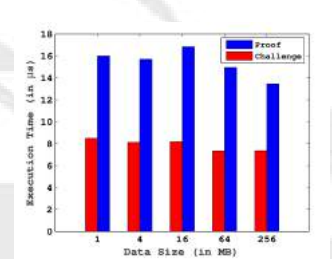
Graph1: Reliability Metric: pairs (12, 12) & (12, 10) has lowest PDL, NOMDL and highest recoverability among all pairs.



Graph2: Storage Efficiency and Overheads: Encoding pair (12,12) achieves high reliability and (10,5) provides the high efficiency and low storage overhead.



(a) Small Files



(b) Large Files

Graph3: Execution Time of Challenge Generation and Integrity Proof Operations during Verification: verification operation takes constant time in microseconds ranging between 7 - 16 μs.

Reference Links

Research Team

- 1. Investigation of Optimal Data Encoding Parameters based on User Preference for Cloud Storage in IEEE Access. Impact Factor 4.640. https://ieeexplore.ieee.org/document/9067840
2. Reliable Verification of Distributed Encoded Data Fragments in the Cloud in Journal of Ambient Intelligence and Humanized Computing. Impact Factor 4.594 (2019) (Accepted)

Prof. Sateesh Kumar Peddoju
Mr. Vikas Chouhan
Mr. Ramakrishna





Android Malware Detection Using Machine Learning

Executive Summary

Android operating system is one of the most popular smartphone operating system in the market. Android is open source mobile platform, Developers can develop and upload Android applications on Google play store or other third party markets. The open source nature of android raises serious issues related to user data privacy and security. Due to the increasing popularity of Android platform, most of the malware developers are targeting Android users.

At IIT Roorkee, We developed static, dynamic and hybrid detection models for Android malware detection. To develop malware detection models, a huge dataset of malicious and benign Android applications are used for feature extraction, model training and testing. We collected a dataset of malware and benign applications and applied reverse engineering approach to extract the features from applications which are required to distinguish malware applications from benign. During the feature engineering, many features were identified which are important for model to classify malware and benign Apps, Some of the useful features are PERMISSIONS, API CALLS, OPCODE, INTENTS etc. We trained the SVM, DT, and KNN models using extracted features and achieved an accuracy of 89.4% with precision 90.2% and recall 86.3%.

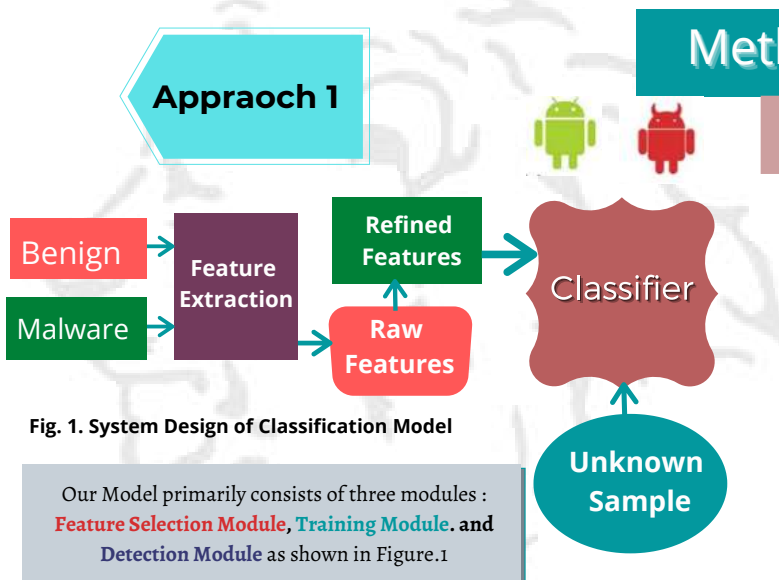


Fig. 1. System Design of Classification Model

Our Model primarily consists of three modules : **Feature Selection Module**, **Training Module**, and **Detection Module** as shown in Figure.1

Feature selection module
Application features like API Calls, Permissions used, System calls made and device features like battery status, Wi-Fi status, contacts and message access status will be logged.

Training Module
This module makes use of logs from selected features in feature selection module. Training module trains the features using collected logs

Detection Module
Detection Module classifies unknown sample into **malware** or **benign** based on the features

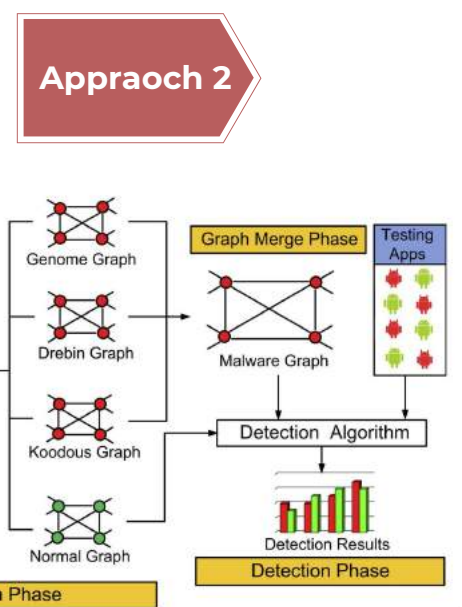


Fig. 2. System Design of PermPair Detection Model [2]

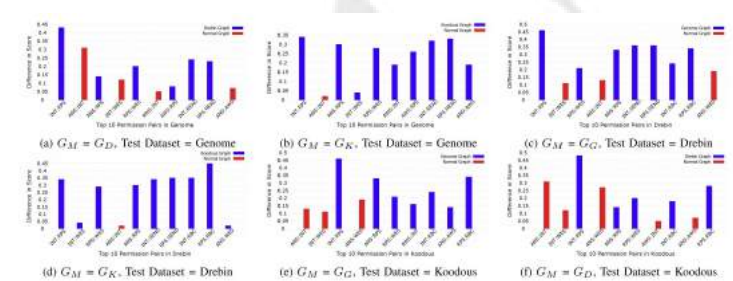


Fig. 3. Malware Dataset Results [2]

Reference Links

1. Hybrid Android Malware Detection by Combining Supervised and Unsupervised Learning "Proceedings of the 24th Annual International Conference on Mobile Computing", <https://dl.acm.org/doi/abs/10.1145/3241539.3267768>
2. PermPair: Android Malware Detection Using Permission Pairs, "IEEE Transactions on Information Forensics and Security", <https://ieeexplore.ieee.org/abstract/document/8886364>
3. NTPDroid: A Hybrid Android Malware Detector Using Network Traffic and System Permissions, "2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)", <https://ieeexplore.ieee.org/abstract/document/8455983/>

Research Team

Prof. Sateesh Kumar Peddoju
Mr. Abdul Kadir
Mr. Anshul Arora
Mr. Ramakrishna





सी डैक
SDC

BOOTH 11



SEGROV

UNDERWATER DRONE

SEGROV is a rugged, compact, remotely operated tethered underwater vehicle which is highly maneuverable and operated by a pilot onboard a vessel, floating platform or on proximate land. It carries multiple payloads like cameras, lights, manipulators and various other sensors for surveillance, navigational and inspection purposes.

Features

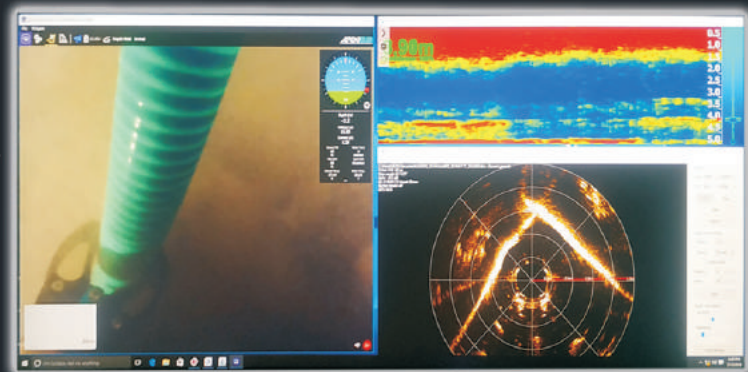
- High performance versatile light work class ROV
- Rugged, compact & portable
- Modular open structure framework, low drag profile
- High maneuverability with 4DOFs
- Scalable architecture
- Rechargeable inbuilt high performance battery pack
- Auto heading & auto depth modes
- 4K video recording



*.. Explore the unknown
where depth is no more the Limit..*

SPECIFICATIONS

Size	620mm x 550mm x 400mm
Weight(in Air)	20 Kg
Construction	Hard anodised Aluminium Grade 6061-T6 and HDPE
Buoyancy foam	Epoxy Coated R-3318 Urethane foam rated to 210m
Maximum rated depth	100m
Maximum forward speed	~ 1m/s (2Knots)
Thruster configuration	6 Thrusters (4 Vectored & 2 Vertical)
Maximum Forward Thrust	14 Kgf
Maximum lateral Thrust	14 Kgf
Maximum vertical thrust	9Kgf
Tether Diameter	7.6mm
Operational Length	120m
Working strength	45Kgf
Breaking strength	160Kgf
Strength member	Kevlar with water block
Buoyancy in water	Near neutral (Slightly positive)
Conductors	8 Nos (4 twisted pairs), 26 AWG
Light Brightness	4 x 1500 lumens each with dimming control
Beam angle	135 degrees with adjustable tilt
Camera 1	1080p digital with 110° field of view and ±90° Pan & Tilt range
Camera 2 (GoPro)	4K Recording
Battery life(Normal usage)	4-6 hrs with 18Ah Li-Po battery pack
Battery life(Heavy usage)	2-3 hrs with 18Ah Li-Po battery pack



STRATEGIC ELECTRONICS GROUP
Center for Development of Advanced Computing

Thiruvananthapuram - 33

For details contact : seg@cdac.in



TrueTraveller

Portable Forensics Tool Kit



TrueTraveller is a portable forensic kit and is a complete solution for performing digital forensics Seizure, Acquisition and Analysis. The kit includes a Laptop installed with digital forensics software tools and an integrated disk imaging hardware solution with battery backup. The kit can be easily carried out for on- location forensic investigations.

Data Acquisition

The kit includes an in-built hardware disk Imaging tool, Truelmager capable of performing high speed data acquisition from SATA, IDE, USB, mini-SATA, micro-SATA hard disks and memory cards. The kit is capable of acquiring Mobile phones using Mobile Check Software and SIM card using SIMXtractor tool.

Image Verification and Destination Disk Sterilizing

The Imaging hardware tool performs hashing of source disk using MD5, SHA1 and SHA2 hashing algorithms, formatting and wiping of destination disk. It also provides image file write verification facility.

Strong Casing with Efficient Packaging

The unit is cased in a rugged, watertight carrying case which protects Laptop, Hardware tools, Software CDs and cables by providing individual permanently fitted carry pouches and trays for each component. The case has individual pouches for drives, tools and cables. The case has built-in connectivity ports for interfacing different storage media. The unit has specially designed areas for power distribution.

Features

- ▶ Easily portable kit with Trolley support
- ▶ Disk imaging hardware tool capable of performing multi-tasking
- ▶ SATA & USB ports for interfacing destination media
- ▶ Includes Write Blockers for SATA, IDE, USB disks
- ▶ Includes adapters for IDE, memory cards, m-SATA & μ -SATA disks
- ▶ Includes Win-LiFT for Live forensics and Net Force Suite for Network forensics
- ▶ Includes CyberCheck Suite for Disk Image Analysis and Advik for CDR Analysis
- ▶ Includes hardware dongle for SIM card seizure and acquisition
- ▶ Includes portable printer, scanner, camera, screw driver set ,torch, Faraday bag and anti-static covers



**PARAM SHAVAK
DL GPU**

In recent time the popularity of Deep Learning is fuelled by major factors such as recent advances in machine learning and signal/information processing research, big data problems, artificial intelligence, lowered cost of computer hardware and drastically increased chip processing abilities with general-purpose graphical processing units (GPGPUs). The advancements in these fields have enabled deep learning techniques to move up to next level by effectively exploiting complex, compositional nonlinear functions, to learn distributed and hierarchical feature representations, and to make effective use of both labelled and unlabeled data.



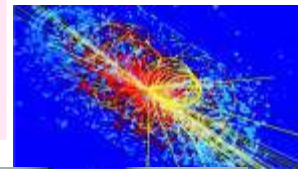
PARAM SHAVAK DL GPU

C-DAC's Deep Learning development - supercomputer in a box, "PARAM SHAVAK DL GPU System" is exclusively designed for academic institutions and research organizations that employ GPU accelerated deep learning techniques for machine learning applications, big data problems, computer vision, speech recognition, natural language processing, life sciences and artificial intelligence. Equipped with x86 based latest Intel processor, 64 GB RAM, 8 TB storage, Nvidia Pascal architecture based co-processing technologies

(P5000/P6000) and software development environment (with Deep Learning GPU accelerated libraries and SDK). This brings innovative and groundbreaking technological approaches to high-end computing on table top platform and does not require costly data center infrastructure. With Nvidia Pascal architecture inside, the system delivers unprecedented performance upto 25 TeraFLOPS of single precision performance for deep learning workloads and enhanced application scalability.

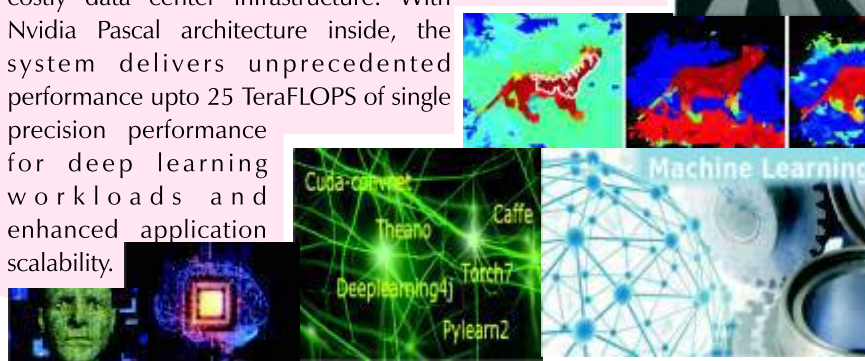
Novelty

PARAM SHAVAK DL GPU appliance provides end to end solution for deep learning, starting from latest hardware, GPU accelerated software development environment, application support, training and tutorials to nurture and satisfy needs of the end users.

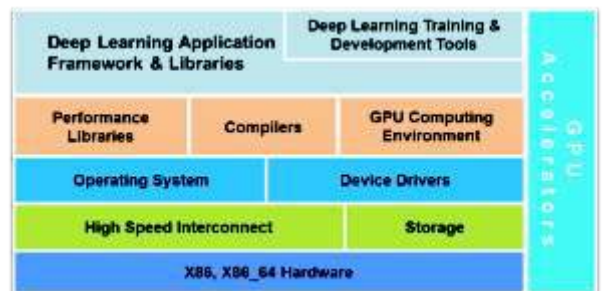


Skill Development

PARAM SHAVAK DL GPU appliance shall enable the country create and develop skills (capability building) to meet industry demands, with a capacity of solving multi-disciplinary grand challenges in science and engineering that employ deep learning techniques. This shall be a boon to the academicians/scientists/industry who want to simulate their research work onto deep learning enabled systems to get desired results.



Architecture



**प्रगत संगणन विकास केंद्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING**

सी-डैक इनोवेशन पार्क, स. न. 34/ब/1, पंचवटी, पाषाण, पुणे - 411008, भारत
C-DAC Innovation Park, S. No. 34/B/1, Panchavati, Pashan, Pune - 411008, India

फ़ोन / Tel: +91-20- 25503547 / 323, फैक्स / Fax : +91-20 -2569 4084

Website: www.cdac.in email : paramshavak@cdac.in



AMRITA
VISHWA VIDYAPEETHAM

BOOTH 12





Innspark Solutions Private Limited

Name and Description

Innspark Solutions Private Limited focuses on research and development of innovative products for enterprises, built by leveraging our unparalleled knowledge in the fields of Cyber Security, Artificial Intelligence and Machine Learning. Innspark Solutions Private Limited was established as an entity under the administrative support of Amrita University to facilitate further development of the technologies and solutions for creating enterprise grade products from the R&D outcome

Our experience in the field of R&D has helped us to bring out world class indigenous, innovative and enterprise grade products across various sectors such as Cyber Security, Healthcare, Transportation etc. Various indigenous products developed across these sectors includes Big-Data driven SIEM solution, SOAR platform, Threat Intelligence, Netflow Generator, DNS security, CDR/IPDR analysis, Vehicle tracking solutions,

Remote health monitoring solution and Biometric authentication systems. We provide the industry's most well respected Security Auditing Services including Vulnerability Assessment and Penetration Testing, Security Auditing of Enterprise Networks, etc. Innspark also has a dedicated security operations team which has expertise in Incident response and threat hunting and is available 24 x 7 for helping the clients safeguard their digital infrastructure.

Abstract about the Products

Big-Data driven SIEM Solution

Innspark Solutions developed and supports our Big Data-driven SIEM solution, which is plugged in with our unmatched and highly curated threat intelligence feed, SOAR and UEBA analytics. Innspark's SIEM solution is extremely, and easily, scalable, and can provide unparalleled visibility into the networks of even the largest of all data centers. Innspark's SOAR platform comes bundled with our SIEM solution, and has a multitude of real world inspired playbooks integrated out of the box. Innspark SIEM solution offers unparalleled 24x7x365 days support by an expert security operations team for helping the clients to safeguard their Intellectual properties and confidential information.

Innspark SIEM is equipped with the functionality that will safeguard even the remote workforce by several innovative authentication mechanisms and also by providing extensive reporting of each of the employees. It is also equipped with an



Innspark Solutions Private Limited

indigenous smart response engine which helps the clients to mitigate a threat in their entire infrastructure with ease. Innspark SIEM will help in augment, compliment and orchestrate the day to day activities of SOC thus removing the pain point of analysts and letting them concentrate on the major incident response tasks.

It is also equipped with an automated vulnerability and exploitability scanner which will alert on the vulnerability status of each of the assets and presents its scope of exploitability which helps in mitigating the threats to a larger extent. In 2020, no threat can be left unnoticed since the landscape of current threats are not only causing loss to the government or enterprise, but are also from state sponsored attackers or are highly organized one. Thus having an Innspark SIEM which provides unparalleled visibility into each of the assets is a must for securing your organization.

Innspark SIEM is available in a one-of-its kind-pricing model with no hidden costs and ensures that even startups with a small digital footprint can keep their infrastructure safe and secure, without exhausting their security budget.

Supporting Links

www.innspark.in

Contact Us

INNSPARK SOLUTIONS PRIVATE LIMITED

Address : CP/XII/482, Clappana PO Karunagappally, KOLLAM - 690525,
Kerala, India

Phone : +91 476-2804550

Mobile : +91 62386-0944

Email : info@innspark.in

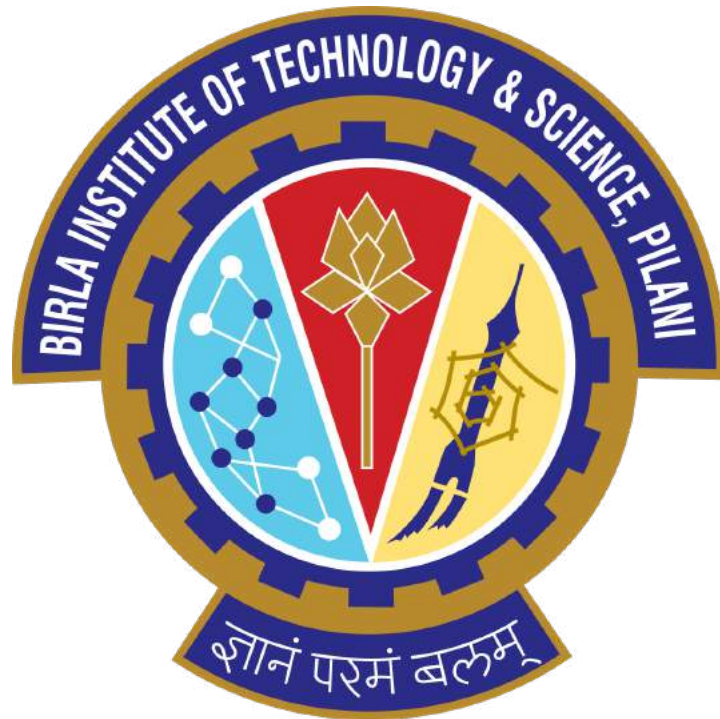


BOOTH 13



PAFST

Predictor and Analyzer of Failure and Security Threats



Developed at Birla Institute of Technology and Science, Pilani

Description:

PAFST is a tool that combines attack trees and fault tree formalisms to obtain a rich plethora of qualitative and quantitative security. The results help organizations ascertain an optimal maintenance strategy and prioritize defence resources to vulnerable assets.

Abstract:

Cyber physical systems, like power plants, manufacturing units and data centers must meet high standards, both in terms of safety (i.e. absence of unintentional failures) and security (i.e. no disruptions due to malicious attacks). Critical infrastructures such as water, electricity that provide society with essential services cannot afford downtime or unavailability of services. However, in the recent past, several security and maintenance incidents have occurred highlighting the need for a more proactive and predictive approach to failures. For example, the 2012 blackouts was the largest ever recorded power outage in history. It affected 620 million people, crippling other dependent services such as metro services, intercity trains etc. Hence it is vital for organizations to adopt measures to predict and nullify such failures.

To this end we present a tool that combines attack trees and fault tree formalisms to obtain a rich plethora of qualitative and quantitative security. The results we obtain help security practitioners identify vulnerable assets, optimize their maintenance strategy, and reduce overall downtime and associated failure costs.

Technically, our approach is realized via the price time automaton model checker Uppaal SMC, providing several advantages over earlier attack tree analysis methods. In particular, we handle more complex gates, including the sequential-and and -or gate, modeling important temporal dependencies between attack steps. Additionally, our trees can include shared subtrees, modeling situations where one action affects multiple avenues of attack. We also support more realistic cost structures.

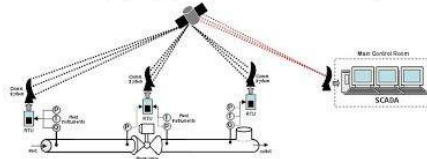
Motivation



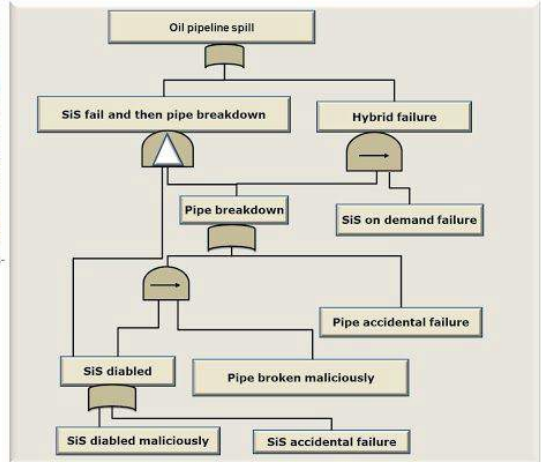
Step 1. Construct an attack-fault tree (AFT)



Trans-Alaska pipeline system (Source of the image: https://en.wikipedia.org/wiki/Trans-Alaska_Pipeline_System, last accessed on 26-09-2017)

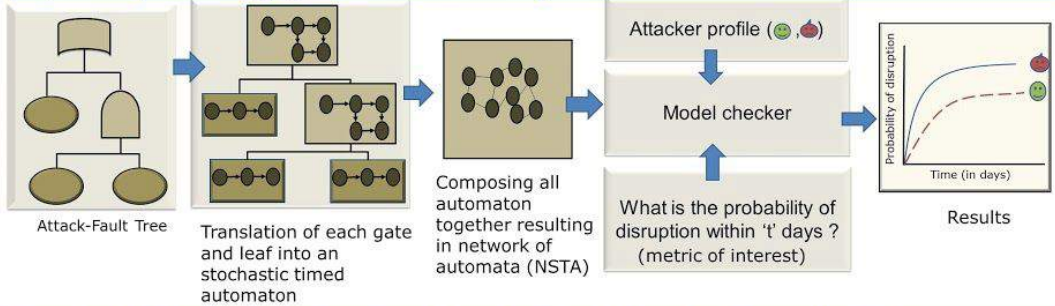


Pipeline transport operations (Source of the image: https://en.wikipedia.org/wiki/Pipeline_transport, last accessed on 26-09-2017)

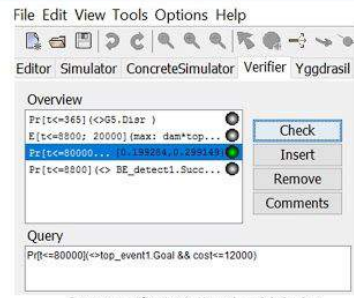
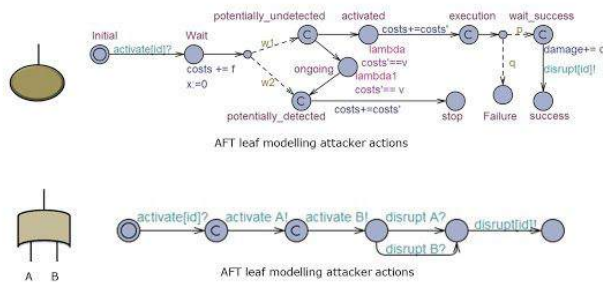


Attack-Fault tree modelling the oil spill in a p

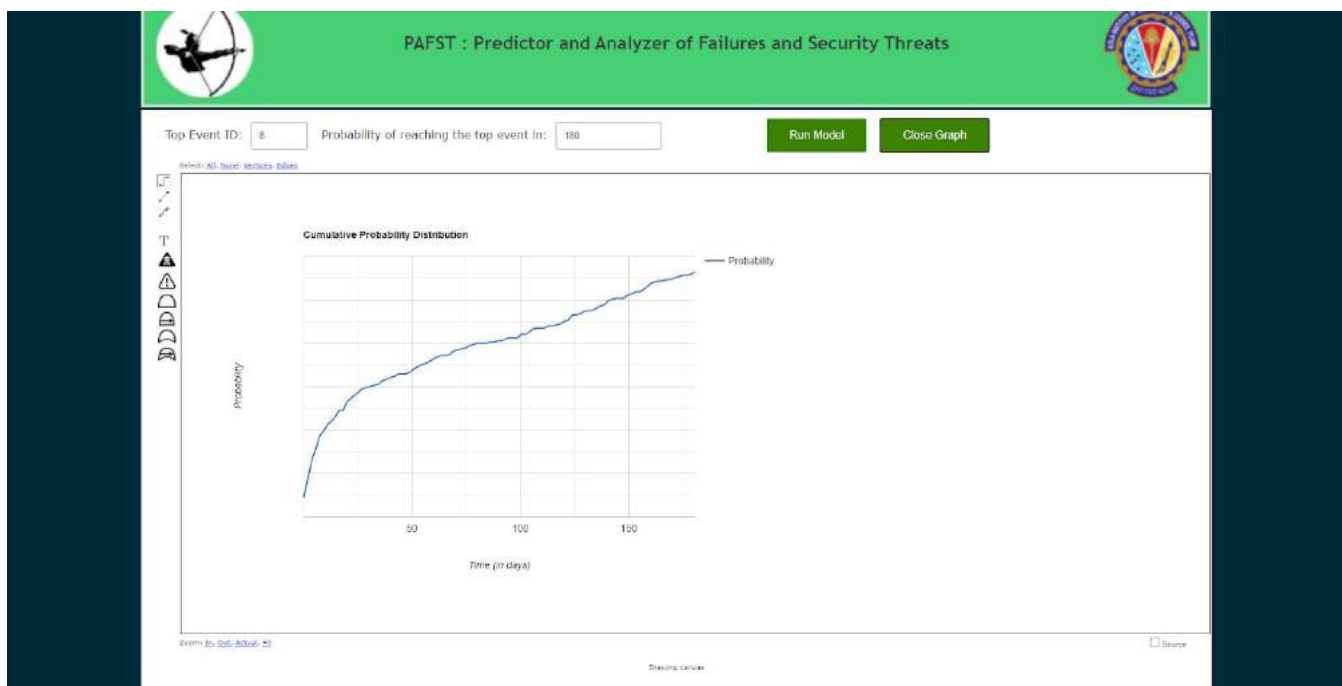
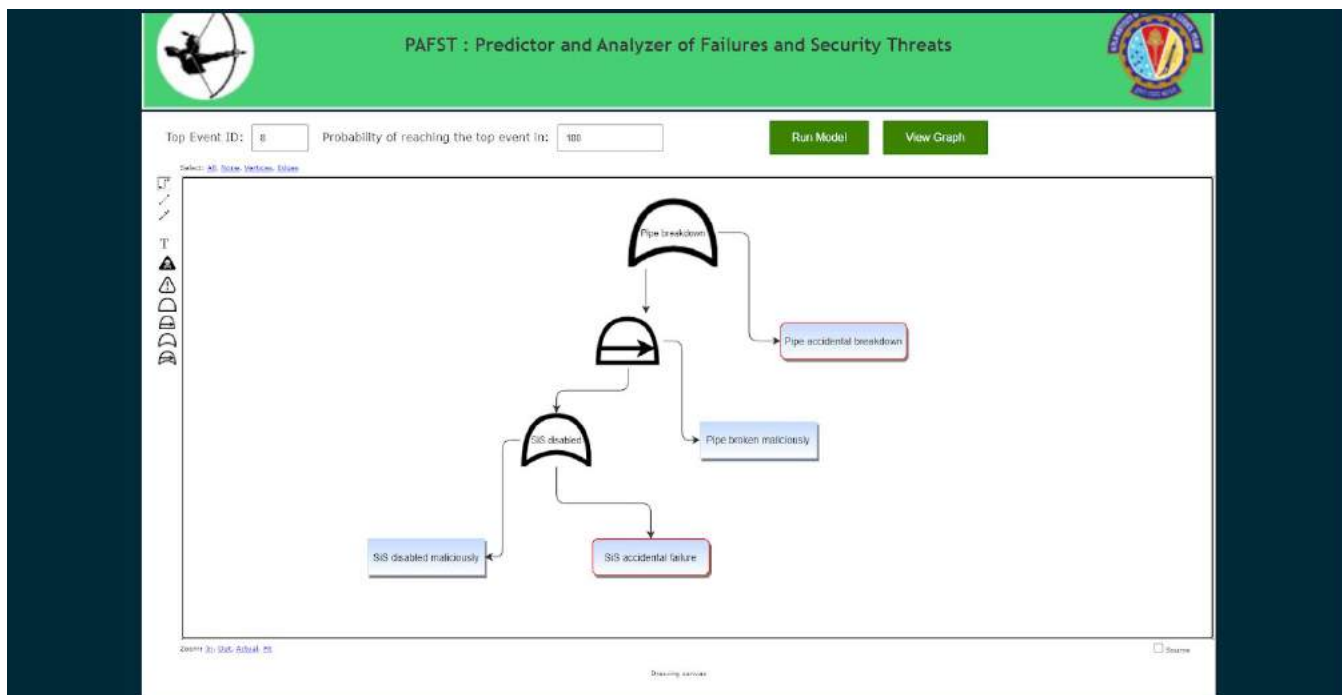
Step 2. Compositional aggregation of AFT leaves and gates



Example of Stochastic timed automata models and metrics of interest fed into model checker



Sample images demonstrating the working of the tool and results



Developer & Contact:

Dr. Rajesh Kumar

PhD, Assistant Professor,
Department of Computer Science & Information Systems
Birla Institute of Technology & Science, Pilani.

Email: rajesh.k@pilani.bits-pilani.ac.in

Office: +91-1596-515-756

Siddhant Singh

BE. Computer Science
Birla Institute of Technology & Science, Pilani.

Email: f2016144@pilani.bits-pilani.ac.in

Rohan Kela

BE. Computer Science
Birla Institute of Technology & Science, Pilani.

Email: f2016822@pilani.bits-pilani.ac.in



BOOTH 14





Secure Network Access System

Description:

SNAS is an indigenously developed integrated network security appliance developed by Bhabha Atomic Research Centre (BARC). It consists of multiple network security components like Network Admission Control, Dynamic endpoint-aware policy enforcement advanced firewall, network monitoring system, endpoint monitoring and usb-device management.

Abstract:

Secure Network Access system (SNAS) is an indigenously developed integrated network security appliance. SNAS secures any enterprise network by intelligently sensing security threats and responding to them automatically. SNAS provides end point security policy compliance by taking policy based decisions regarding who gets admission into the network and with what level of network access privileges.

SNAS identifies the “who, what and where” of the end systems connected in a network. It can identify almost everything on the network – the devices, their operating systems and the applications running on them. SNAS combines the features of a perimeter firewall with those of an endpoint security solution to provide a bird’s eye view of the entire network as well as detailed information about each entity connected to it. SNAS can be easily configured to suit the network security requirements of different types of enterprises.

SNAS can be deployed in enterprise networks to replace the existing firewalls between intranet segments (LAN) and various demilitarized zones and WAN. SNAS will ensure that the devices in the user segment comply with security policy and all internal network attacks are identified and mitigated. The SNAS security suite provides a comprehensive solution for mitigation of internal and external attacks.

SNAS has got many network security components such as:

Network Admission Control (NAC) module of SNAS makes sure that end-systems are allowed to access network services only if they are in compliance with the security policy defined for them. Even after policy compliance, they are only allowed to access services designated for them. Regular post-connect checks ensure that the connected systems remain in healthy state and comply with the enterprise network security policy

Host Aware Security Policy Enforcement Dynamic Firewall module supports advanced firewall features like Traffic Prioritization, Bandwidth Shaping, Rate Limiting, Profile based Logging and Log Analysis. The firewall is host aware as the



Secure Network Access System

firewall rules are only present when the systems are live and meeting the enterprise network security policy. SNAS Network Visualization module provides a mechanism to monitor and manage the various network devices and end-systems present in the network. It overlays the network map with the security state of the devices providing various types of views.

SNAS detects and isolates Rogue (unknown) end systems in the network. It can also detect and prevent the merging of networks which are supposed to be isolated.

SNAS also monitors the end-systems present in the network and identifies any behavioural changes taking place in the network. This information can be used to identify any anomalies in the network.

USB based devices like pen-drives, external hard-disks, cameras, internet-dongles etc. pose risks of data-theft and virus propagation. SNAS can ensure that only authorized USB-based storage devices are used on an end-system. The movement and usage of USB devices within the network is also tracked.

SNAS supports deployment in High-Availability mode to provide seamless access to network services.

Currently there are more than 30 deployments of SNAS across the country

Supporting Links:

<http://www.barc.gov.in/publications/nl/2014/spl2014/pdf/paper04.pdf>

<https://www.thehindubusinessline.com/companies/ecil-launches-router-security-solution-under-license/article23072792.ece>

<http://workshop.nkn.in/2012/Document/slides/day2/SNAS%20by%20Gigi.pdf>

Contact Details:

Shri Gigi Joseph,
CISO & Head, GNS, Computer Division, BARC

Email : gigi@barc.gov.in

Phone : 022-25593555



BOOTH 15





C.I.S.H

Abstract:

Deep-learning (DL) has become the striving research focus for detecting anomalies effectively in recent times. Deep neural-networks learn the data patterns at multiple-levels, corresponding to varied number of abstraction filters specified based on the nature of data. This learning style of neural-networks flagged the idea of optimizing conventional networking problems and build enhanced solutions to distinguish anomalous packets from the overall network traffic. The mandatory requirement of voluminous data for training DL models counter as a major drawback for getting executed in network peripherals hosting NIDS with minimal memory and processing power.

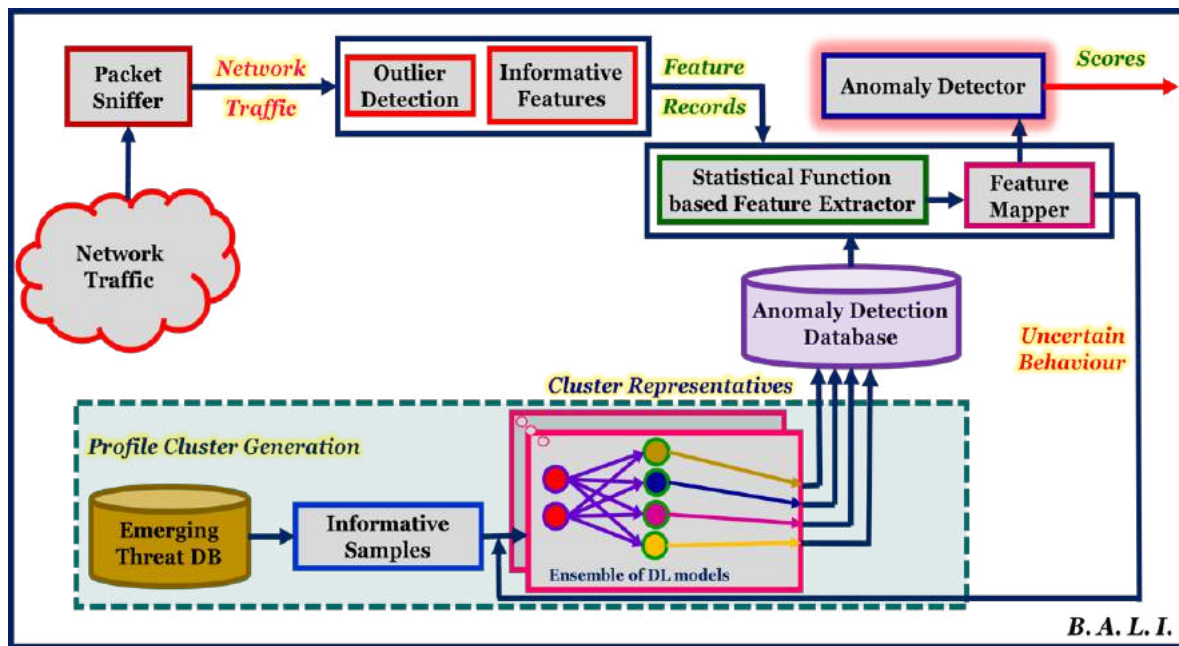
More importantly, next generation firewalls that implements enhanced intrusion detection modules alongside the conventional packet filter procedure, executes the learning procedure in a supervised manner that demands manual packet labelling on a timely basis. Thus, CISH develops Behaviour based Anomaly-detection over Log files and Inbound traffic (BALI) for detecting anomalies on the network traffic in an unsupervised manner. Feature-extraction module in addition to the ensemble of DL models effectively tracks the underlying patterns of each network channel.

The current version of neural-network based PnP-network intrusion detection framework (BALI) executes efficiently on a 64-bit machine, over which resource usage analysis is under study. The NIDS targeting cyber-physical systems is in its prototype stage which is funded by Ministry of Electronics and Information Technology (MeitY), Government of India.

Related



C.I.S.H



Related Publications of Principle Investigator Supporting the Research Area
URL: Prof. V. S. Shankar Sriram

Contact Details:

Prof. V. S. Shankar Sriram

TATA Communications Chair Professor of Cyber Security Associate Dean-Computer Science and Engineering & Incharge IT Services School of Computing, SASTRA Deemed University

Email : sriram@it.sastra.edu

Mr. Sujeet S. Jagtap

Junior Research Fellow Centre for Information Super Highway (CISH) School of Computing, SASTRA Deemed University

Email : sujeetjagtap@sastra.ac.in



BOOTH 16





CSIR-4PI

CSIR Fourth Paradigm Institute
(CSIR-4PI), Bangalore

It is well known that cyberspace consists of a wide variety of malicious activities. These activities typically include massively Distributed Denial-of-Service (DDoS) attacks, automated worm propagations, Internet wide port-scanning, etc. In fact, cyberspace has a well-organized attack network with millions of compromised hosts, which can be used to launch powerful cyber attacks. In order to recruit new hosts to the attack network, already compromised hosts in the attack network regularly scan the global Internet Protocol (IP) address space. Internet-wide scanning typically generates a special type of network traffic known as unsolicited network traffic.

Unsolicited traffic is a potential resource for cyber security dynamics inference. CSIR Fourth Paradigm Institute (CSIR-4PI), Bangalore, with its Cyber Security Research and Observation (CySeRO) team, is actively researching on various aspects of unsolicited traffic for remote inference of cyber security dynamics. Towards this, the Institute is developing a 'Network Telescope' framework.

In another activity CSIR-4PI is also actively involved in design and development of algorithms and protocols for security and privacy of futuristic technologies such as connected vehicles, especially Vehicular Ad-hoc Networks (VANET). In this direction the team have developed lightweight rekeying mechanism based on permutation parity machines (PPM) for a dynamic multi-casting environment and deep learning based safety aware pseudonym changing mechanism for privacy enhancement.

The major challenge in working in such futuristic concepts is the lack of appropriate infrastructure to test the algorithm. This has limited the research in the area of connected vehicle at least by Indian researchers. Also to develop machine learning based algorithms, data availability becomes a major concern in the absence of real-time implementation. Keeping this in mind CSIR-4PI has initiated activities to create capacity as well as capability to carry out research in Intelligent Transportation System.

A VANET simulator has been engineered (only for research community) using various open source solutions for testing and analyzing security and privacy related algorithms and is in the process of being made available as a Docker image through GitHub. The simulator is capable of testing new algorithm for both IEEE and ETSI standards. Also, further to carrying out simulations in the absence of a possibility for real time implementation, CSIR-4PI has setup India's first vehicular test-bed based on Duckietown (a road infrastructure with a number of robotic toy vehicles). This has the capability to test various vehicular algorithms and protocols.



CSIR-4PI

CSIR Fourth Paradigm Institute
(CSIR-4PI), Bangalore



Contact Details:

Address: CSIR Fourth Paradigm Institute NAL Belur Campus, Bangalore-560037

Email : head@csir4pi.in



BOOTH 17





Secured Embedded Architecture Laboratory

Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur

In the past decade, the field of hardware security has grown into a major research topic, attracting intense interest from academics, industry and governments alike. Secured Embedded Architecture Laboratory (SEAL) as part of the Department of Computer Science and Engineering at IIT Kharagpur is dedicated to fostering a vibrant hardware security community in India and beyond. We are committed to building and strengthening the technical expertise and awareness about hardware design of cryptographic algorithms, testability and side channel analysis of hardware design, hardware intellectual property protection, Hardware Trojans, machine-learning assisted hardware security, microarchitectural and system security, privacy preserving smart grid system, automotive security, and design of Physically Unclonable Functions (PUF) for device fingerprinting while empowering like-minded individuals to pursue their interests in academic, enterprise or entrepreneurial undertaking at the same time.

As the security research community in India is growing beyond theoretical cryptography, our main objective is to make people around academics and industry aware of the basic and fundamental research that is happening in the area of applied cryptography and hardware security at IIT Kharagpur and develop necessary skills to mitigate the existing threats.

Over more than 10 years, SEAL has developed an absolutely state-of-the-art laboratory for hardware security research at IIT Kharagpur. We have experimental setup to launch power attacks, EM-based attacks, fault attacks using laser station, row hammer attacks on X86 and RISC based platforms, various cache timing attacks, focused ion beam (FIB) station for detection of IC counterfeit, temperature and humidity chambers for characterization of PUFs, real-time simulator setup with phasor measurement units and Phasor Data Concentrators for smart grid systems. Driven by the motto of our Institute, "Dedicated to the Service of the Nation", the SEAL group focuses on research that has high impact value either to the Indian society or the security community worldwide.

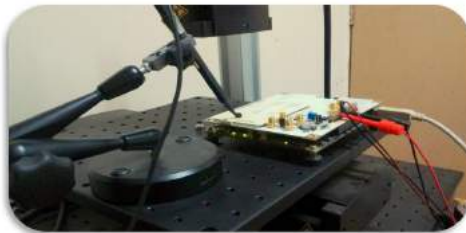
We have been actively working with various governmental agencies by delivering state-of-the-art high impact research projects and also as a consulting partner and undertaken and successfully delivered a number of research projects with leading multinational companies. We strongly believe that collaboration is an important aspect in research, which helps in exchanging interesting ideas and culminate high-impact research output. We actively collaborate with leading universities and researchers and have won various awards and recognition from different organizations due to the quality and impact of the work done. SEAL at IIT Kharagpur has a pool of highly motivated and talented M.S. and Ph.D. scholars who have been working on diversified research



Secured Embedded Architecture Laboratory

Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur

areas in hardware security. SEAL also boasts of highly accomplished group of alumni who hold positions as research scientists, post-doctoral researchers and faculties at prestigious universities and companies all over the world. We have published more than 150 research papers in several top-tier conferences such as EuroCrypt, CCS, NDSS, CHES, FSE, DAC, DATE, PKC, AsiaCCS, HOST and journals such as IEEE TIFS, IEEE TDSC, IEEE TC, IEEE TCAD, IEEE TVLSI, IEEE ESL, ACM TOPS, ACM TECS etc. SEAL has incubated a start-up "ESP-Research" (esp-research.com), at the entrepreneur's park (SEAL, IIT-KGP) to deliver security solutions and consultations regarding threats on hardware security and crypto-engineering.



Contact Details:

Address : Secured Embedded Architecture Laboratory, Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India- 721302

Email : debdeep@iitkgp.ac.in / debdeep@cse.iitkgp.ac.in



BOOTH 18





AIMSCS

C R Rao Advanced Institute of Mathematics, Statistics and Computer Science , University of Hyderabad Campus

- The CR Rao Advanced Institute of Mathematics, Statistics and Computer Science (AIMSCS) was established in honor of the legendary Statistician Padma Vibhushan Prof. C. R. Rao FRS, with the sole aim of promoting quality research in the areas of Mathematics, Statistics, Computer Science and related areas.
- The Institute has initiated action to create Centres of Excellence in the area of Cryptography and Cryptanalysis to carry out Research, Development, Consultancy and Training.

Centre of excellence in Cryptography and Cryptanalysis:

The Centre of Excellence in Cryptology at CR Rao AIMSCS, University of Hyderabad Campus, Hyderabad, is being setup. The goal of this centre is to work on advanced areas of Cryptography & Cryptanalysis and related fields.

Activities

- The research faculty & research fellows in the group will carry out research in the advanced areas of Cryptography & Cryptanalysis and Cryptanalysis using High Performance Computing.
- The centre has also undertaken several Crypto and Information security projects for various GOI Agencies / Public Sector Enterprises. These includes Research and training in Cryptography, Lattice based Cryptology, Post Quantum Cryptology, SAT/SMT solver-based Cryptanalysis, Design of Symmetric Key ciphers, Random test suites and Design of Security protocols. We have published 80+ research papers, prepared many technical reports and developed software tools in the area of Cryptology. In the institute, at present 6 faculties, 25 research scholars and 5 adjunct faculties are working in theory and practical applications in Crypto and Information security areas.

Workshops/Conferences:

We have conducted three international conferences in association with CRSI and IACR that includes INDOCRYPT 2019, INDOCRYPT 2010 and SPACE 2016. We have also organized several National workshops which include Algebraic Cryptanalysis; Lattice based cryptography, SMT solver-based cryptanalysis, code-based cryptography and recently National Workshop on Cryptology, Sept 5-7, 2018. We also conducted several training programmes in the area of Cryptology to Intelligence agencies, Govt of India.



AIMSCS

C R Rao Advanced Institute of Mathematics, Statistics
and Computer Science , University of Hyderabad Campus



Contact Details:

Prof. D.N.Reddy, Director

C.R.Rao Advanced Institute of Mathematics, Statistics and Computer Science (AIMSCS)

Phone : +91 40 23012324, +91 40 23013118 (Tele fax)

Email : reddydn@gmail.com / directoraimscs@gmail.com /
director@cr Raoaimscs.res.in

Web : www.crraoaimscs.in



GSFC
UNIVERSITY
EDUCATION RE-ENVISIONED

BOOTH 19



Smart system for Bot detection by analyzing DNSRR queries

Abstract

With the growth of fast flux and domain flux technology the need of bot detection system for randomized Command & Control botnet traffic required. This paper proposes methodology for bot detection based on DNSRR (Domain Name Server Resource Record) queries. The proposed algorithm tested with DETER testbed and CIC and ISCX datasets. The results are very encouraging.

Introduction

There are various malicious software's exists that can be injected into systems for various attacks from eavesdrop the information to Denial of Service. Botnet are known as one of the most serious software attack today [1, 2].

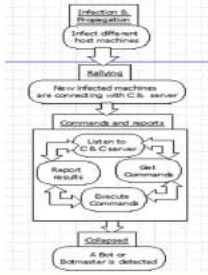


Fig. 1 - Botnet life cycle

Fig. 2 - (a) centralized; (b) decentralized

Type of Botnet	C&C Protocol/Channel	Structure	Strength	Weakness	Examples
IRC	IRC [8]	Centralized	Communication with low latency. Real time control over bots. Flexible.	Each bot must know the IRC server, port, and communication channel to be of any use to the botnet. With detection of IRC server, the entire botnet can be detected and collapsed [9,10]	Spybot, Agobot, O'Tbot, SDDot, etc.
HTTP	HTTP	Centralized	The communication between bots use normal HTTP traffic so difficult to detect presence of bot	No real time control over bots, if Web server will be shutdown entire botnet will be collapsed [2]	Clickbot, Bobax, etc.
P2P	Peer to Peer communication, Self-defined	Decentralized	No single point of failure, robust	Communication with high latency[11]	Nigacha, Storm, etc.

Table 1 - Hierarchy of botnet components.

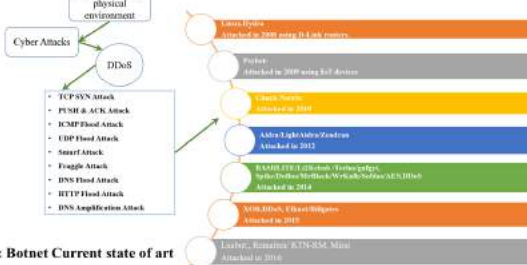


Fig. 3: Botnet Current state of art

UNDERLYING PRINCIPLE

SNo	Scenario	Detail	Sno	Research Paper	Work	Limitation
1	DNS of C&C server at initial Phase	At the initial assemble phase of botnet, DNS of C&C server needed for creation of assembly of bots with C & C server	1	Jones [3]	The technique used bot programs for identification bots	Possible to identify only known Footprints
2	DNS transient during initiating bot activation	For triggering bots for performing various malicious activities C & C server instructions are embedded in DNS transient	2	Cooke [4]	Proposed model based on structure of bots, monitoring IRC communication and C & C Activity	Not able to detect encrypted traffic
3	DNS of new C & C server	Due to some failure or lost connection with C & C server, bots needs to be connected with other C & C server.	3	Barford [5]	Analysis of software used for infecting bots.	Identify only known specifications of software
4	Assembly Problem and Botmaster	The main challenge is to rallying the infected hosts. Botmaster uses DNS for rallying infected hosts in the network to make them portable and hidden.	4	Rajab [2]	Analysis of structural and behavioral aspects of botnet	Dependent on structure of botnet
5	C&C Server Migration	To avoid detection by intrusion detection systems Botmaster instructing bots to shift or connect to other command control server.	5	Dagon [6]	Based on DNS traffic which include DNS request rate and DNS density	Not able to identify poisoned DNS
			6	Binkley [9]	Anomaly based technique for detecting IRC based botnet	High false positive rate
			7	Rajachandran [10]	Based on DNSBL (DNS Black List) reconnaissance activity of Botmaster	High false positive rate
			8	Houising [11]	Monitor DNS traffic to detect bots on the basis of group activity	If use of DNS poisoning not able to work

Table 2 few scenarios based on DNSRR queries.

Table 3 research work for bot detection techniques.

BotDNSRR query	Timestamp and IP address accessed to C & C Domain name	Bot structure activity	DNSRR query type
BotDNSRR query	Only bots send queries to C & C domain server which normally fixed and all bots sends request in group or easily identifiable.	All the Bot machines connected in Botnet resembles similar behavior. In botnet all bot machines act and migrate together in group and at similar timestamp.	Temporary and simultaneously Use DNSRR for C & C servers.
NonBotDNSRR query	The normal, authorized DNS queries triggered from NonBot machines and at random rate.	All the NonBot machines behave in random fashion. Do not use DNSRR.	Continuously and randomly.

Table 4: difference between BotDNSRR query traffic and NonBotDNSRR query traffic

Challenges
C & C communication based on underlying Protocol
C & C communication traffic is similar to normal traffic
C & C communication is encrypted
There may be less number of Bot communication in the network
C & C servers changing properties over time

Table 5 - challenges in detecting bots in network traffic.

PROPOSED SOLUTION

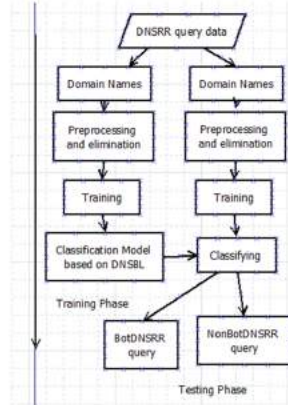


Fig. 4: Working flow of proposed model

Proposed mathematical equations:

Flow feature equation

$$f_e = \langle \text{DNS}, s_{ps}, d_p, TS, DN, l_s, l_e \rangle \langle \text{features} \rangle$$

Query structure equation

$$q_s = \langle \text{dir}, \text{size}, \text{DN}, l_s, l_e, \text{data} \rangle \langle \text{structure} \rangle$$

Classification and clustering analysis: query feature vector v(q)

$$v(q) = \langle PT, ql, ql_1, ql_2, \dots, ql_n, qlb \rangle \langle \text{query vector feature} \rangle$$

Distance function d(u,v) for different flow:

$$d(u,v) = (1/W)d_{ss}(u,v) + (1/W)d_p(u,v) + (1/W)d_q(u,v)$$

Where weighting factor W will be considered:

$$W = \begin{cases} 3 & \text{if } u.PT = \text{DNS} \wedge v.PT = \text{DNS} \\ 2 & \text{else} \end{cases}$$

The distance equation for query data size dq(u,v):

$$dq(u,v) = \frac{|u.qb - v.qb|}{\max(u.qb, v.qb)} \cdot u.PT = \text{DNS} \wedge v.PT = \text{DNS} \\ 0, \text{ else}$$

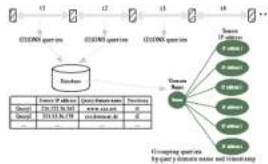


Fig. 5: Insert_BotDNSRR_Query

```

Insert DNS-Query (Qi) = DNS-queries between time t+1 and t
1 Ai ← Array for DNS queries
2 DWi ← Request domain name of Qi
3 IF DWi is not in Ai
4 insert(DWi, Ai)
5 IF IPi is not in IPi
6 insert(IPi, IPi)
7 ELSE IF IPi is not in IPi
8 cnti ← size of IPi
9 cnti = cnti + 1
10 insert(IPi, IPi)
11 ENDIF
12 ENDFOR
End of Insert-Bot-Query
    
```

Fig. 7: Insert_BotDNSRR_Query

$$S = \frac{1}{2} \left(\frac{C}{A} + \frac{C}{B} \right) \text{ if } (A \neq 0, B \neq 0)$$

Similarity equation

```

Delete-NonDNSRR-Query
1 FOR k = 1 to n
2 W, T ← Whitelist, size threshold
3 IF (DWk is in W) OR (DWk >= cnt < T)
4 delete(DWk, Ai)
5 delete(IPk, IPi)
6 ENDIF
7 ENDFOR
End of Delete-NonDNSRR-Query
    
```

Fig. 6: Delete_NonBotDNSRR_Query

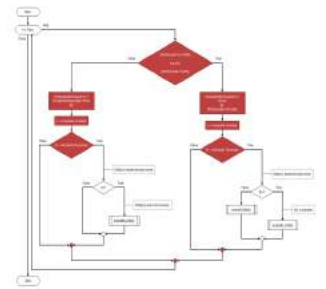


Fig. 8: Detect_C&C_Migration

Results

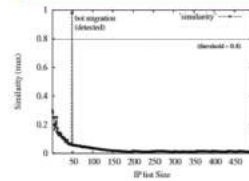


Fig. 9: Similarity of IP addresses

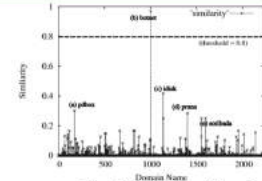


Fig. 10: Similarity of Domain names

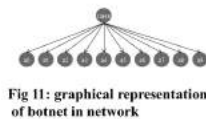


Fig. 11: graphical representation of botnet in network

Conclusion

The proposed methodology able to detect bots effectively without concerning underlying architecture and communication traffic pattern. The scope of proposed system is to work on offline detection of bots. In future we will validate proposed approach with real setup of systems with infected machines to extend this approach for real time detection of bots using DNSRR queries.

References

- B. Saha and A. Gairola, "Botnet: An overview," CERT-In White PaperCIWP-2005-05, 2005.
- M. Rajab, J. Zarfoss, F. Mourou, and A. Terzis, "A multifaceted approach to understanding the botnet phenomenon," in Proc. 6th ACM SIGCOMM Conference on Internet Measurement (IMC'06), 2006, pp. 41–52.
- N. Iuella, A. Hackworth, "Botnets as a vehicle for online crime," CERT Request for Comments (RFC) 1700, December 2005.
- Honeynet Project and Research Alliance, Know your enemy: Tracking Botnets, March 2005. See <http://www.lamneyet.org/papers/bots/>.
- G. Schaffer, "Worms and Viruses and Botnets, Oh My! : Rational Responses to Emerging Internet Threats," IEEE Security & Privacy, 2006.
- E. Cooke, E. Jahani, and D. McPherson, "The zombie roundup: Understanding, detecting, and disrupting botnets," in Proc. Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUIT'05), 2005, pp. 39–44.
- A. Ramachandran and N. Feunster, "Understanding the network-level behavior of spammers," in Proc. ACM SIGCOMM, 2006.
- Z. Zhu, G. Lu, Y. Chen, Z. J. Fu, P. Roberts, K. Han, "Botnet Research Survey," in Proc. 32nd Annual IEEE International Conference on Computer Software and Applications (COMPSAC '08), 2008, pp. 96–97.
- J. B. Grizzard, V. Sharma, C. Numery, B. B. Kang, and D. Dagon, "Peer-to-peer botnets: Overview and case study," in Proc. 1st Workshop on Hot Topics in understanding Botnets, 2007.
- P. Wang, S. Sparks, and C. C. Zou, "An advanced hybrid peer-to-peer botnet," in Proc. 1st Workshop on Hot Topics in understanding Botnets, 2007.



BOOTH 20





Indian Institute of Technology Jammu

Description:

The Indian Institute of Technology Jammu was inaugurated on 6th August 2016, and welcomed the first batch of students into the campus in Paloura, Jammu. In the initial phases, the establishment of IIT Jammu was done under the mentorship of IIT Delhi. In 2018, IIT Jammu shifted the primary operations to the Main Campus in Jagti, Nagrota. The State Government, Jammu and Kashmir has provided land for the establishment of a permanent campus of the Indian Institute of Technology in Jammu, which consists of 400 acres. Currently the Phase 1 A of the main campus, spread across 25 acres, is operational. Phase 1 B and 1 C are undergoing construction. We have 27+ MoUs with Industry, Government and Academic organizations at national and international level to foster growth in the area of research, technology development and skilled learning.

Abstract of Research Work: Dr. Brudheshwar

Internet-of-Things Security: Fingerprinting and Access Control

The IoT paradigm has resulted in a multitude of devices becoming part of our networking ecosystem. An IoT device is a device that is designed to perform a specific task and has the ability to communicate over the network. From smart bulbs to industrial control systems, the applications are numerous. Given this scenario, the security of a network deploying IoT devices is very important. An IoT device might exhibit malicious behavior or spy on the privacy of users. Therefore, understanding the device behavior and constraining its actions are critical to ensure the reliability and security of the rest of the network.

This work explores these two facets in detail, i.e., device fingerprinting and access control. The device fingerprinting approach examines the network traffic of a given IoT device and attempts to learn the behavior of the device. If the behavior of the device deviates from the standard security baseline of the network then an access control mechanism restricts such activities of the device. We consider the attribute-based access control model (ABAC) in our work and explain how such a model can establish the necessary security boundaries.



Secure Network Access System

Protecting Web Users from Cyberthreats: Phishing Detection and Machine Learning

Phishing websites pose a significant threat to web users. A phishing website masquerades a legitimate website and attempts to steal sensitive credentials of the users. Some websites also act as malware delivery agents. The phenomenon is continuing unabated since the last two decades and there appears to be new waves of threats and opportunities for attackers every other year. Machine learning approaches have been quite popular to detect phishing websites. A machine learning approach examines a corpus of collected data sets and tries to build a learning model to identify a phishing website.

However, the dynamic nature of these attacks imply that as time goes by the older machine learning approaches will perform poorly and will not adapt to the newer wave of attacks. In our work, we explore partially data agnostic approaches to detect phishing websites. Specifically, we focus on designing features that reflect the nature of the phishing websites. Our approach has been successful in achieving 99.7% accuracy in experiments on laboratory and live data.

Dr. Gaurav Varshney

One-time period debit/credit cards invention states to generation of on demand virtual cards/physical cards having predefined expiry and transaction limit entered by user, making it more user specific and this invention proposes a way of performing transaction with NFC tags/token + PIN/Secret even at ATMs to withdraw cash or for payment at online websites using methodology like Web NFC, etc. Whenever the card compromises or its validity expires the user can generate a new one time period card themselves and use it virtually as a QR and create a physical NFC card/token using the smartphone App. The method through which POS machines and websites perform transactions via one time period card is also discussed in this invention.



Get in touch with us

Address : 3rd Floor, NASSCOM Campus, Plot No. 7-10, Sector 126, Noida, UP -201303
Email : ncoe@dsci.in **Contact :** +91 2598 987451