SUNDAR KRISHNAN

PhD, CISSP, CISM, CDPSE, PMP, ITIL (F), Six Sigma Black Belt | Dr.Krishnan@Outlook.com | **Ph: 832 812 8105**

August/10/2022

PROFESSIONAL SUMMARY

PhD in Digital and Cyber Forensic Science with research focus in security, risk and privacy of data and digital forensic evidence. Career experience of 26 years includes 18 years in mid-management positions in Cybersecurity and Information technology and 3 years of teaching. Passionate to transfer industry gained knowledge through teaching and mentoring students in addition to undertaking development of academic Cybersecurity programs involving Penetration Testing, Defense, Incident Forensics, Privacy and Risk management.

EDUCATION

PhD in Cyber and Digital Forensics (Cyber/Computer Forensics and Counterterrorism)	Sam Houston State University, Huntsville, Texas, USA	Aug/2018 - Aug/2022

Dissertation: *Sentiment and Behavioral Analysis of case suspects, Financial Fraud detection of suspects from forensic evidence, Sexual Harassment detection of suspects from forensic evidence*

Master's in Digital Forensics (Cyber/Computer Forensics and Counterterrorism)	Sam Houston State University, Huntsville, Texas, USA	Jan/2013 - May/2015

Academic project: *Design, Build and Deploy a working SCADA lab for vulnerability assessments, penetration testing & incident forensics*

Master's in Computer Applications	Bharathiar University, India	Aug/1999 - Dec/2002
Bachelor of Science (Major in Electronics)	Bangalore University, India	Jun/1992 - May/1995

CERTIFICATIONS

- Certified Information Systems Security Professional **(CISSP)**
- Certified Data Privacy Solutions Engineer **(CDPSE)**
- Project Management Professional (**PMP**)
- **Six Sigma Black Belt**
- **ITIL** v3 Foundation
- Certified Information Security Manager (**CISM**)
- SEI-CMMI **ATM** (Assessment Team Member SCAMPI-B)
- Microsoft Certified Professional in 70-562 (**MCP** .NET 3.5 and Web application)
- Certified in Industrial Control Systems – Cybersecurity, ICS-CERT, DHS

RESEARCH INTERESTS

Security, privacy, risk, and analytics (Machine Learning/Neural Networks) in

i. Digital Forensic Evidence
ii. Medical Device CyberSecurity
iii. Industrial Security of SCADA (Supervisory Control and Data Acquisition) devices

TEACHING EXPERIENCE

1. • CS 3310 Unix (Fall 2022) – Angelo State University
2. • CS 4320-01 Computer and Network Security (Fall 2022) – Angelo State University
3. • CS 4320-02 Computer and Network Security (Fall 2022) – Angelo State University
4. • CS 4390 Cryptography (Fall 2022) – Angelo State University

5. CSTE 1330 Introduction to Computers (Spring 2022), undergraduate class, Sam Houston State University
6. CSTE 1330 Introduction to Computers (Fall 2021), undergraduate class, Sam Houston State University
7. COSC 1436 Programming Fundamentals (Spring 2021), undergraduate class, Sam Houston State University
8. COSC 1436 Programming Fundamentals (Fall 2020), undergraduate class, Sam Houston State University
9. COSC 1436 Programming Fundamentals (Spring 2020), undergraduate class, Sam Houston State University
10. COSC 1436 Programming Fundamentals (Fall 2019), undergraduate class, Sam Houston State University
11. Designed and setup a fully functional SCADA/HMI lab at Sam Houston State University with zero funds to assist students in Industrial Cybersecurity (Pen Testing, Defense, and Incident Forensic exercises). Reached out to SCADA equipment vendors to donate equipment.
12. Advised CCDC teams at Sam Houston State University by discussing with CCDC lead on possible competition scenarios. Volunteered as a CCDC White Team member (judge).
13. Part-time instructor between 1996 to 2002 – Taught classes programming languages like C++, C, Java, Oracle, Powerbuilder, VB 5.0, Crystal Reports, etc. at NIIT, APTECH and SPAN India (All Franchises closed since 2002).
14. Mentored many Information Technology professionals during my career in industry.

CONFERENCES, SEMINARS & WEBINARS

1. International Conference on Advances in Computing Research (ACR), Program committee member, Cybersecurity Engineering and Mobile and Cloud Computing track
2. IEEE International Conference on E-Learning in Industrial Electronics (ICEIE), Technical Program Co-chair
3. 7th International Symposium on Digital Forensic and Security (ISDFS 2019) conference presentation of "SCADA Testbed for Vulnerability Assessments, Penetration Testing and Incident Forensics"
4. Technology and Cybersecurity Panel, Center for Russian, East European, and Eurasian Studies, University of Pittsburgh
5. Webinar on SCADA and HMI Security in InduSoft Web Studio
   YOUTUBE Link: https://www.youtube.com/watch?v=kBcXCM7Y3vA
6. Sam Houston State University PhD program Seminar on *Security, Privacy and Steganographic Analysis of FaceApp and TikTok*

PROFESSIONAL ORGANIZATIONS

1. IEEE Student Member
2. Information Systems Audit and Control Association (ISACA) – Houston Chapter
3. Information System Security Certification Consortium (ISC^2)

PEER REVIEWER – JOURNALS & CONFERENCE

1. Journal Review Board member - International Journal of Information Security Science - http://www.ijiss.org
2. IEEE International Symposium on Technology and Society (ISTAS) 2019

3. Journal Review Board member - International Journal of Security (IJS), CSC Journals
4. 7th International Symposium on Digital Forensics and Security (ISDFS) 2019
5. 8th International Symposium on Digital Forensics and Security (ISDFS) 2020
6. 9th International Symposium on Digital Forensics and Security (ISDFS) 2021
7. International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME) 2021
8. International Conference on Electrical, Computer and Energy Technologies (ICECET) 2021

AWARDS & RECOGNITIONS

1. Best Reviewer Award- 2020 International Journal of Security (IJS)
2. Recognized for serving as Secretary to IEEE WG P2834 "*Standard for Secure and Trusted Learning Systems*"

WORK EXPERIENCE

Assistant Professor of Computer Science, Cybersecurity — **Angelo State University, San Angelo, TX** — **Aug 2022 – till date**

- Taught classes assigned by the Department Chair

Graduate Research Assistant, Security/Forensics Researcher in Cybersecurity and Digital Forensics — **Sam Houston State University, Huntsville, TX** — **Aug 2018 – Aug 2022**

- Worked on Smartphone, Disk and Network Forensics
- Taught classes assigned by the Department Chair
- Authored and co-authored peer-review publications, abstracts, and conference presentations
- **Dissertation Research focus areas: eDiscovery, Electronic Stored Information, Digital Forensic Evidence – Security, Machine Learning, Neural Networks and Forensics**

Information Security Summer Intern — **Sam Houston State University, Huntsville, TX** — **June/2021 - Aug/2021**

- Worked with the SHSU Information Security Team a part of my PhD program required Internship.
- Advised the Information Security Team on development of policies and standards based on DIR TX - Security Control Standards Catalog
- Advised the Information Security team on existing control gaps with the current SHSU security posture

Information Security Operations Manager — **Methodist Le Bonheur Healthcare, Memphis, TN** — **Mar/2017 - June/2018**

- Responsible for managing the information security operations across the organization thereby keeping an eye on organization's digital security footprint.
- Responsible for the enterprise security program in the areas of risk management, vulnerability management, incident response, security operations, governance, compliance, and incident forensics.

- Key areas of responsibilities.
    - Cybersecurity Strategy and Implementation across all facets of the security discipline
    - Ensuring strategic alignment of Cybersecurity with business objectives
    - Manage the Cybersecurity Operations team consisting of five security analysts
    - Manage a team of Network security resources managing enterprise firewalls, remote access and VPN
    - Manage enterprise network security
    - Managed and advise on medical device security.
    - Manage the Vulnerability Management Program
    - Manage endpoint encryption process
    - Manage SIEM with assistance of MSSP (overseeing 65+ FTEs)
    - Managed the Cybersecurity Incident Response Program overseeing cyber incidents response, containment, resolution, and forensics.
    - Participated in key IT Security and Privacy Governance teams
    - Managed Application Security and hardening
    - Managed the vulnerability program and penetration testing
    - Maintained all Cybersecurity tools and technology of the organization.
    - Ensured Cybersecurity stays on the organizational leadership vision.
    - Assisted on Network Segmentation and Isolation
    - Assisted with monitoring internal and external policy compliance.
    - Assisted with audits of policies and controls continuously.
    - Coordinated on new technology adoption like cloud services with an eye on minimizing risk and attack surface.
    - Assisted with Security Risk Management, Risk Acceptance and Risk Mitigation
    - Assisted with identifying remote access solution for vendors
    - Worked with different departments in the organization to reduce overall security risk.
- Key accomplishments and implementations
    - Deployed QRadar (SIEM) to monitor critical assets.
    - Established SIEM continuous monitoring program with MSSP
    - Redeployed vulnerability scanner across almost 100% cross-platform servers and network gear.
    - Managed deployment of MFA/2FA against Virtual Private Network (VPN) and Enterprise Reverse proxies.
    - Managed Local Admin Privs revocation of users and systems across enterprise.
    - Managed deployment of CyberArk EPM to manage user's privileges on endpoints.
    - Managed Privilege Account Management solution POC/POT

- Performed security gap analysis a needed
- Assisted with promoting security awareness, trainings and conducting internal presentations.
- Created security polices standards and operating procedures as applicable.

Information Systems Security Manager **University Health System, San Antonio, TX** **Nov/2015 - Mar/2017**

- Responsible for implementing the information systems security program from ground-up across the organization.
- Responsible for the enterprise security program in the areas of risk management, vulnerability management, incident response, security operations, governance, and compliance.
- Key areas of involvement, implementation, and improvement.
  - Security Strategy and Implementation across all facets of the security discipline
  - Ensuring strategic alignment of Security with business objectives
  - Manage the Cyber Security Operations Center
  - Introduce and manage the Vulnerability Management Program
  - Manage the Cyber Security Incident Response Program
  - Participation in key IT Governance teams
  - Tuning and tightening the server patching process
  - Implemented Risk Management, Risk Acceptance and Risk Mitigation standards
  - Defined Asset Management thereby laying foundation for identifying critical assets and data.
  - Performed security gap analysis
  - Scoping the Penetration testing exercise, vetting external pen-test vendors.
  - Promoting security awareness, trainings and conducting internal presentations.
  - Creating polices/standards, introducing controls and governance.
  - Defining critical data criteria, its handling, protection, and storage.
- Management and administration of staff responsible for security tools such as SIEM, vulnerability management/configuration management, malware detection, file integrity monitoring, multi-factor, web content filtering, and others.
- Manage a team of security professionals (Security Analysts and IAM security provisioning administrators).
- Manage operations support of endpoint disk encryption software (Sophos), Websense (email, web and DLP), Netbotz security cameras, BYOD/MDM, IAM/IDM, Malware sandboxing, RSA SA, PHI and PII discovery, device hardening.

- Oversee various Cybersecurity initiatives while working with cross-functional teams (Applications, developers, vendors, clinicians, project managers, end users, helpdesk, networking, storage, middleware, and server teams)
- Research and recommend the appropriate industry standards to alleviate security threats thereby contributing to information/Cybersecurity continuous improvements and strategic planning.
- Manage the IAM Team functional tracks: User Compliance, Provisioning/De-provisioning, Privileged User Management.
- Communicate with IT leadership on security gaps, governance, risk exposure and health of IT security program.
- Conduct and communicate Cybersecurity status reviews with various stakeholders.
- Perform Security Risk Assessments against operations/program/projects.
- Designed, developed, and implemented Security Risk Assessment toolkit based on NIST and HIPPA frameworks.
- Oversee security incidents to containment and closure, impact to business, complete RCAs, and investigative reports.
- Monitor the organization's vulnerability-scanning program for internal and external-facing hosts.
- Oversee security newsletters publications, awareness trainings and security related stakeholder communications.
- Ensured all approved policies related to change control, security, and segregation of duties are strictly adhered to.
- Ensured adherence to privacy and security policies in accordance with HIPPA.
- Stay abreast of technology, security trends and Industry best practices by evaluating new solutions and products.
- Performed estimation, ROI, Risk assessments, change control and process improvements on security projects.
- Provide direction, constructive feedback, and technical guidance to staff. Set goals, priorities, review and evaluate work, and conduct performance reviews.
- Ensure vendor security compliance to business agreements.
- Reported and worked under the CISO of the organization.
- Proposed and established various security groups and committees focusing on key problem areas and gaps.
- Key accomplishments:
    - Upgrade of Forcepoint Websense to 8.1
    - Implement email processing and spam Filtering in Forcepoint (Websense) TRITON-EMAIL
    - Evaluate and deploy a replacement BYOD/Mobile Data Management solution

- Configure PHI eDiscovery on Websense [Endpoints and network]
- SOPHOS Safeguard upgrade (end point protection via disk encryption)
- Finalize, Rollout and Implement Incident Response Plan (IRP tabletop exercises in progress).
- Rollout/Implement IAM solution (access provisioning maintaining a degree of SOD. Final phase in progress.)
- Upgraded DLP monitoring across 8000+ endpoints
- Implemented endpoint monitoring through CISCO FireAMP agents across 8000+ endpoints.
- Implemented email Phishing awareness and education solutions using Forcepoint (Websense) TRITON-EMAIL
- Implemented malware threat processing in the cloud using Forcepoint (Websense) TRITON-EMAIL
- Upgrade of digital forensic tools like EnCase.
- Security questionnaires for vendors and project managers during system acquisitions and project delivery.

Principal Consultant, Security Intelligence Analytics & Assurance **Wipro Ltd, Houston, TX, USA** **Jun/2011 - Nov/2015**

- Worked as a Principal Consultant in the Enterprise Security Solutions (ESS) practice as part of the Security Intelligence Analytics Assurance (SIAA) team.
- Provided consulting services (advisory services, transformational solutions, and managed security services) around end-to-end security and compliance solutions globally across industry verticals.
- Led a team of five resources based in Houston, TX.
- Led and manage Public Key Infrastructure (PKI) and Single Sign On (SSO) implementation, QRadar log archival to AWS.
- Consulted on Multi-Factor Authentication Implementation and improvement of Patch Management process driven by vulnerability assessments.
- Conducted security exercises focused on penetration tests and vulnerability assessments against websites, routers, switches, and databases with technical teams spread across Geos.
- Managed incident management and investigations at Security Operations Nodal Center, ensuring security events are investigated and remediated for 24x7 continuous operations by support team.
- Advised senior management by identifying critical security gaps and recommended risk-reduction solutions.
- Responsible for integrating processes between Identity and Access Management (IAM) systems with the client's AD.
- Interpreted information security vulnerabilities, risks, policies, and procedures to Application and infrastructure teams

- Responsible for Identifying, analyzing, conduct triage, containment, resolution, monitoring, and reporting of information security incidents.
- Analyzed logs from webservers, services, databases, applications, and log data to determine security weaknesses.
- Monitored enterprise user access provisioning (LDAP and AD) processes and related jobs.
- Proactively protected the availability, integrity, confidentiality, and privacy of business data.
- Planned and implement application security by developing security solutions, directing system control development and access management, monitoring, and evaluation.
- Performed Security Risk Assessments against operations/program/projects
- Conducted security code reviews.
- Participated in vendor management, SLAs, and security governance.
- Participated in Disaster Recovery exercises.
- Advised technical teams in designing and implementing security solutions and technologies.
- Document and maintain security standards, guidelines, and procedures

Technical Lead / Project Manager **Science Applications International Corp (SAIC), Houston, TX, USA** **Sep/2003-Jun/2011**

- Led and managed full development lifecycle projects of various sizes and complexities. Coordinated the timeliness and quality of work effort for the team onshore and offshore).
- Managed a team of five resources based in Houston, TX, one resource based in UK and ten resources based out of India
- Managed escalations for project related issues, challenges, or questions from project team. Played a role of Lead architect with team members at onshore and offshore. Provided technical and process guidance to the project and support team.
- Played a role of Operations Coordinator (technical) on the ADM service delivery program involving 250 applications as on portfolio. Provided 24/7 support on various applications as a SME (Subject Matter Expert).
- Worked as a technical lead on projects developing code and mentoring teams across Geos. Have programmed project modules in .NET, MVC and SharePoint technologies
- Managed systems responsible for Active Directory Account Creation, Group Memberships
- Designed, developed, and deployed .NET project for change management for the Terminal Transport and Marine business.
- Implemented and managed web security certificates on webservers for various customers.

- Designed, developed, and deployed a .Net project for change management for the downstream Pipeline business.
- Designed and developed .NET alternatives to legacy HR applications due for retirement in 2013 using MVC and JQuery.
- Designed and developed SSIS packages for data integration across Data centers.
- Enhanced a .NET console application that caters to the sync between enterprise AD, HR data and Exchange Mailboxes.
- Owned Root Cause Analysis and Problem Management for managed services provided to customer.
- Served as escalation point for application support and troubleshooting, provides guidance and direction in resolution of escalated issues around application or system problems.
- Served as the first line of escalation for domain technology issues that cannot be resolved by tiers one and two support.
- Assisted staff developers with code maintenance, unit test and new feature development using the .NET platform
- Setup and maintain cloud-based Windows web and application servers utilizing Window Server 2008 & IIS 7.5.
- Setup and manage the application database utilizing Microsoft SQL Server 2008. This included configuring maintenance plans, database backups and data maintenance.
- Worked on RFP/Bid process for projects along with the PMs providing technical consultation around .NET technologies, MOSS(SharePoint), SQL Server (DB design, SSIS, SSRS, SSAS programming) and Oracle (DB Design and programming).
- Kept development team and management informed about applicable security issues as they relate to web applications or applicable government regulations (e.g., SOX, Microsoft coding best practices).
- Worked with applications that integrate into Customer SharePoint environment using .NET technologies. Supported applications built around asp, .NET, SQL Server, and Oracle technologies for customer. Provided support for the Customer Rebill system involving Autosys jobs, DTS packages and OLAP Cubes.
- Provided primary support SAP Portal for customer
- Integrated multi-factor authentication systems into an enterprise web application.
- Worked with SSO for SAL Portals
- Worked on application defect investigations and resolution as part of service delivery services
- Worked on mainframe conversion to .NET projects for payroll processing.
- Performed code reviews as part of pair programming and training peers on secure coding practices.
- Performed code maintenance, unit test and new features development using the .NET platform.

- Led and managed full development lifecycle projects of various sizes and complexities.
- Coordinated the timeliness and quality of work effort for the team (onshore and offshore).
- Performed Incident management related to security during ongoing service delivery.
- Presented papers on ROI of application security controls and process improvements
- Participated as Assessment Team Member to evaluate SAIC-India against CMMI process maturity.
- Led ADM program transitions and transformations. Worked on RFP/Bid process for projects.
- Assisted with network setup and configuration, security scanning at SAIC-India during SAIC's India operations rollout.
- Ensured all approved policies related to change control, security, and segregation of duties are strictly adhered to.

Cybersecurity Summer Intern **InduSoft, Invensys (Schneider Electric), Austin, TX** **May/2014 - Aug/2014**

- Participated in internal training sessions to learn the products, services offered by InduSoft, as well as the Industrial Automation market where the company plays a role.
- Created documents and presentations about best practices in cyber security, based on the products and services offered by InduSoft.
- Collaborated with the QA team to identify current and future cyber security vulnerabilities in the products offered by InduSoft.
- Conducted custom presentations for technical internal teams (development, QA, technical support), describing best practices and concepts that must be applied to improve the cyber security reliability of products and services provided by the company.
- Conducted custom presentations for marketing/sales internal teams, describing advantages of the InduSoft products and services regarding cybersecurity, so InduSoft can properly convey the main concepts to customers.
- Conducted presentations to current and potential customers describing best practices in cyber security and demonstrating how InduSoft products and services follow such procedures.
- Elaborated a Cyber Security guideline manual and presentations for HMI/SCADA applications, focused on the products offered by InduSoft.
- Elaborated case scenarios and test procedures focused on Cyber Security reliability for the QA department.
- Improved the InduSoft's product quality assurance and testing team's awareness about good practices in cyber security and, consequently, the credibility of the company in the market.
- Directly reported to the VP, Consulting services on daily progress.

Worked as Software Developer/Programmer at various Information Technologies companies in India between June' 1995 to Sept' 2003

FRAMEWORKS AND CONTROLS

♦ NIST – Cybersecurity ♦ OWASP ♦ ISO 27001 ♦ PCI ♦ HIPPA ♦ SEI-CMMI ♦ COBIT

AREAS OF EXPERTISE

- PHI and PII protection
- HIPPA, Privacy
- Risk Management
- Security Audits
- Change Management
- Identity & Access Management
- Asset Management
- Machine Learning
- Penetration Testing
- Business Continuity
- Disaster Recovery
- Application Security
- Continuous Operational Processes Improvement
- Cyber Kill Chain
- PCI Security
- Asset Hardening
- Vulnerability Management
- Incident Management
- Digital Forensics
- Project Management
- Root Cause Analysis
- Six Sigma Methodology
- Patch Management
- Biomedical Devices Cybersecurity
- Information Security Governance
- Threat Modelling
- Program Transitions
- Industrial Cybersecurity
- Malware Sandboxing
- Security policies and standards
- Cybersecurity Awareness Trainings
- Critical Data Management
- Legal and eDiscovery Security

TECHNICAL SKILLS

- **Access controls/ IdM/IAM**: NetIQ, Sailpoint
- **Analytics:** Machine Learning, Feature selection
- **Data Loss Prevention (DLP):** Forcepoint(Websense) 8.1, McAfee
- **eMail monitoring & anti-phishing:** Forcepoint (Websense) 8.1, Proofpoint, PishMe
- **eDiscovery:** Relativity, Exterro, MS Office
- **Endpoint Monitoring**: Carbon Black, FireAMP
- **Endpoint Disk Encryption**: Sophos SafeGuard, McAfee, Bitlocker
- **Endpoint Security**: McAfee, Windows Defender, Symantec
- **Endpoint Privilege Management**: CyberArk (Viewfinity) EPM
- **Encryption**: SSL/TLS, Microsoft Public Key Infrastructure (PKI)
- **Forensics tools**: FTK Imager, Paraben, Encase, Ida, FTPPro, Autopsy, OllyDb, Encase
- **Industrial Control Systems Protocols**: MODBUS TCP/IP, DNP 3.0, OPC, KOYO, CodeSys ARTI
- **Load Balancers**: F5, Netscaler
- **Medical Devices Security**: Firewall and network segmentation of Drager Fusion Pumps, Imaging systems and more
- **Mobile Device Management (BYOD):** Airwatch, MaaS360, Openpeak Toggle, MobileIron
- **Multifactor authentication:** Duo, RSA
- **Network Sniffing tools**: Wireshark, BurpSuite
- **Network Security**: Palo Alto Firewalls, Juniper Firewalls, F5 Load Balancers

- **Operating System:** Windows, Linux Distros, Unix, Kali Linux, Samurai Web Testing Framework
- **Penetration Testing:** Metasploit, SQLmap, BurpSuit, Aircrack custom scripts
- **Privilege Account Management:** CyberArk PAM (familiarity)
- **Privilege Access Management:** CyberArk EPM
- **Programming**: Python, .NET, C#, VB .NET, C++, C, VisualC++, JavaScript, VBScript, ML.NET and more
- **RDBMS & related**: Oracle, SQL Server, MYSQL, SSIS, SSRS and more
- **Security Information and Event Management (SIEM)**: QRadar, RSA Secure Analytics, familiar with Splunk
- **Secure Network, IDS/IPS logging and monitoring**: IPSEC, SSL, SSH, Snort, RSA Secure Analytics
- **SCADA/HMI**: Indusoft Web Studio
- **SSO**: Ping Federate, Form-fill
- **Threat Intelligence feeds**: ThreatConnect, IBM Threat Intelligence, Palo Alto Wildfire
- **Virtual Platforms:** VMware, Virtual Box
- **Vulnerability Tools:** SQLMap, NMAP, WMAP, OpenVAS, Nessus, Nikto, Nexpose, Qualys, OWASP
- **Vendor Management platforms:** SecureLink, CyberArk
- **Web Application Firewalls**: Imperva Secure Sphere, F5

PUBLICATIONS

Research Profile: https://scholar.google.com/citations?user=ziladycAAAAJ&hl=en

1) **S Krishnan**, ABMR Islam, C Varol, N Shashidhar , A Novel Text Mining Approach to Securities and Financial Fraud Detection of Case Suspects, *International Journal of Artificial Intelligence and Expert Systems*
2) **S Krishnan**, ABMR Islam, C Varol, N Shashidhar, A Novel Text Mining Approach to Sexual Harassment Detection of Case Suspects, *International Journal of Artificial Intelligence and Expert Systems*
3) **S Krishnan**, ABMR Islam, C Varol, N Shashidhar, Sentiment Analysis of Case Suspects In Digital Forensics and Legal Analytics, *International Journal of Security*
4) **S Krishnan**, ABMR Islam, C Varol, N Shashidhar, Analytics in Digital Forensics and eDiscovery Software - DevOps, Opportunities and Challenges, *International Journal of Security*
5) **Sundar K.**, Ashar N., & Qinzhou, L. (2021). IoT Network Attack Detection using Supervised Machine Learning, *International Journal of Artificial Intelligence and Expert Systems*
6) **Krishnan, S.**, Shashidhar, N. (2021). Interplay of Digital Forensics in eDiscovery. *International Journal of Computer Science and Security (IJCSS)*, *15*(2), 19.
7) **Krishnan, Sundar**, and Bing Zhou. (2020). Predicting Crime Scene Location Details for First Responders. *8th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE

8) Neyaz, A., Kumar, A., **Krishnan, S.**, Placker, J., & Liu, Q. (2020). Security, Privacy and Steganographic Analysis of FaceApp and TikTok. *International Journal of Computer Science and Security (IJCSS)*

9) **Krishnan, S.** (2020). Exploitation of Human Trust, Curiosity and Ignorance by Malware. *arXiv preprint arXiv:2002.11805*

10) **Krishnan, S.**, Zhou, B., & An, M. K. (2019). Smartphone Forensic Challenges. *International Journal of Computer Science and Security (IJCSS)*, *13*(5), 183-201.

11) **Krishnan, S.**, Neyaz, A., & Shashidhar, N. (2019). A Survey of Security and Forensic Features In Popular eDiscovery Software Suites. *International Journal of Security (IJS)*, *10*(2), 16.

12) **Krishnan, S.**, Shashidhar, N. (2019). eDiscovery Challenges in Healthcare. *International Journal of Information Security Science*, *8*(2), 30-43.

13) **Krishnan, S.**, Wei, M. (2019, June). SCADA Testbed for Vulnerability Assessments, Penetration Testing and Incident Forensics. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE

14) **Krishnan, S.**, & Chen, L. (2019). Legal Concerns and Challenges in Cloud Computing. *arXiv preprint arXiv:1905.10868*.

15) **Krishnan, S.**, Shashidhar, N., Varol, C., & Islam, A. R. Evidence Data Preprocessing for Forensic and Legal Analytics. *International Journal of Computational Linguistics (IJCL)*

UPCOMING PUBLICATIONS

- Sentiment Analysis of Case Suspects from Forensic Evidence
- A Novel approach to Financial Fraud Detection from Forensic Evidence
- A Novel approach to Sexual Harassment Detection from Forensic Evidence
- Privacy in Streaming Devices
- Wearables Security

REFERENCES

Dr. Qingzhong (Frank) Liu
Associate Professor, Department of Computer Science, Sam Houston State University, Huntsville, TX 77341
Ph: (936) 294 3569 | Email: Liu@shsu.edu

Dr. Narasimha K. Shashidhar
Associate Professor, Department of Computer Science, Sam Houston State University, Huntsville, TX 77341
Ph: (936) 294-1591 | Email: karpoor@shsu.edu

Dr. Bing Zhou

Associate Professor and Chair, Department of Computer Science, Sam Houston State University, Huntsville, TX 77341
Ph: (936) 294-1590 | Email: zhou@shsu.edu