# Saikat Das, Ph.D.

Wichita Falls, TX 76308.
901-265-4415, drsaikatdas21@gmail.com
https://github.com/CSMLGroup
https://www.linkedin.com/in/saikatdasphd/

## Academic Background

**Ph.D.**, Computer Science, University of Memphis, TN — May 2021
**Dissertation:** Detection and Explanation of DDoS attack using Interpretable Machine Learning

**M.Sc.**, Computer Science, University of Memphis, TN — December 2016
**Master's Project:** Collaborative Runtime Monitor as Intrusion Detection System

**B.Sc.**, Khulna University of Engineering and Technology (KUET), Bangladesh — May 2011
**Thesis:** Towards Minimizing the Risks of System Failure

**Certification**, Cisco Network Academy Program, KUET, Bangladesh — April 2011

## Professional Skills

**Tenure Track Assistant Professor**
Midwestern State University, Wichita Falls, TX — August 2021 - Present

- Conduct research; develop trustworthy, advanced cybersecurity systems to improve the early detection of cyber-attacks for applications.
- Designing and teaching courses: Computer Science I, Contemporary Programming Languages, and Web Application Security (Graduate).

**Graduate Research and Teaching Assistant**, — January 2015 - May 2021
Game Theory and Cyber Security Lab, University of Memphis.

- Improved feature selection and designed explainer models using Interpretable Machine Learning.
- Implemented ensemble supervised and unsupervised ML frameworks and analyzed their performances in detecting DDoS attacks; Improved detection accuracy with reducing false alarms.
- Mentored, instructed, and graded for TA courses: Artificial Intelligence, Data Information Knowledge, Computer Organization & Architecture, Programming Language, and Cryptography.

**Cyber Defense Instructor**, Southwest TN Community College, TN — August 2018 - July 2019

- Prepared and designed courses & laboratory materials for the courses: Computer Security, Principles of Info. Assurance, Cyber Defense, Tactical Perimeter Defense, and Computer Applications.
- Improved curriculum for Cyber defense program at SWTCC and increased student enrollments.

**Web Developer Intern**, Pannin Technology LLC, TN — May 2016 - August 2016

- Modified existing eCommerce website to correct errors and improved performances.
- Implemented features like car rotating, merging carts, etc. for FleetSafety3D in Ruby on Rails.

**Senior Software Engineer**, Samsung Electronics, Bangladesh — March 2013 - August 2014

- Analyzed and fixed >300 critical problems for existing Samsung mobile java applications.

- Developed features like push message, timeout lock, wallpaper picker, etc. for java applications.
- Performed post managerial role to ensure high level software solutions.

**Software Engineer**, Evatix Ltd, Bangladesh May 2011 - February 2013

- Implemented eCommerce solutions like product search, list, and mgmt.; related products, frequently bought items, cart, and checkout mgmt.; user, admin and merchant panel, etc.
- Developed several websites for dating, management, and eCommerce in PHP, Zend, JavaScript.

# Research Interests and Accomplishments

### Interpretable Machine Learning (Taxonomy, Comparative Analysis, Feature Selection)

- Proposed a taxonomy of interpretable machine learning methods with building blocks.
- Comparison of recent day interpretable machine learning methods and their associated tools.
- Proposed a novel feature selection approach using IML technique that produced a reduced feature set. A better DDoS detection accuracy is obtained using this feature set.
- An explanation mechanism is designed for detected DDoS attacks using IML. The implementation showed a comparative analysis of explanations from two IML models.

### Machine Learning and Data Science (DDoS Intrusion Detection System):

- Proposed ensemble supervised and unsupervised techniques in detecting DDoS attacks. Implementation of these ensemble frameworks outperformed single model classification.
- Designed an ensemble feature selection mechanism that combines several well-known feature selection methods using majority voting technique.
- The detection accuracy of DDoS attacks increased by at least 5%, and lowest false positive rates are achieved compared to existing work.
- Several datasets, such as NSL-KDD, CICIDS2017, UNSW-15, and HTTP CSIC 2010 in various domains are pre-processed, sanitized, feature reduced and finally the results obtained from the classification models are analyzed to find the best performing models using proposed techniques.

### Cyber Security (Runtime Monitor, Intrusion Detection and Prevention System (IDS), (IPS)):

- Several intrusion detection mechanisms are proposed using Natural language processing, Genetic Algorithm, rule based approach, etc.
- Stealthy False Data Injection attacks are detected in a smart grid using proposed IDSs.
- Detected and prevented DDoS, packet drop and bad data injection attacks in a simulated smart grid using Simulink.
- A collaborative runtime monitoring mechanism is proposed to monitor the system behavior in a collaborative fashion in real time for detecting possible threats. It also has the inbuilt preventive action plans or defense strategies for the countermeasure of these potential attacks.

### Cloud Computing (Moving Target Defense):

- Proposed a stealth migration protocol to transfer an anomalous virtual machine in cloud infrastructure. The implementation certainly obfuscated the migration process from the attackers which provided an extra layer of security.

### Computer Network

- Conducted several research work on network security analysis, vulnerability assessment and data hide from external adversary during virtual machine migration.

# Publications

1. Das, Saikat, et al., "Network Intrusion Detection and Comparative Analysis using Ensemble Machine Learning and Feature Selection" **Revised version submitted** in "IEEE Transactions on Network and Service Management" *(Under Peer Review)*

2. Das, Saikat, et al., "DDoS Explainer using Interpretable Machine Learning" **Submitted** in "2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference" *(Under Peer Review)*

3. Das, Saikat, et al., "Machine Learning Ensemble-Based Intrusion Detection for DDoS Attacks", **Prepared for submission** in "Elsevier Computers & Security"

4. **Das, Saikat**, Mohammad Ashrafuzzaman, Sajjan Shiva, and Frederick T. Sheldon,"Network Intrusion Detection using Natural Language Processing and Ensemble Machine Learning" 2020 IEEE Symposium Series on Computational Intelligence. IEEE, 2020.

5. **Das, Saikat**, Deepak Venugopal, Sajjan Shiva, and Frederick T. Sheldon, "Taxonomy and Survey of Interpretable Machine Learning Method" 2020 IEEE Symposium Series on Computational Intelligence. IEEE, 2020.

6. Agarwal, Namita and **Saikat Das** "Interpretable Machine Learning Tools: A Survey" 2020 IEEE Symposium Series on Computational Intelligence. IEEE, 2020.

7. Ashrafuzzaman, Mohammad, **Saikat Das**, Yacine Chakhchoukh, and Frederick T. Sheldon "Elliptic Envelope Based Detection of Stealthy False Data Injection Attacks in Smart Grid Control Systems" 2020 IEEE Symposium Series on Computational Intelligence. IEEE, 2020.

8. **Das, Saikat**, Deepak Venugopal, Sajjan Shiva, and Frederick T. Sheldon. "Empirical evaluation of the ensemble framework for feature selection in DDoS attack." In 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 56-61. IEEE, 2020.

9. Ashrafuzzaman, Mohammad, **Saikat Das**, Yacine Chakhchoukh, Sajjan Shiva, and Frederick T. Sheldon, "Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning." Computers & Security 97 (2020): 101994.

10. Ashrafuzzaman, Mohammad, **Saikat Das**, Yacine Chakhchoukh, Sajjan Shiva, and Frederick T. Sheldon, "Supervised Learning for Detecting Stealthy False Data Injection Attacks in the Smart Grid", Proceedings of the International Conference on Security and Management, SAM'20, July 2020, Las Vegas, USA. (Accepted)

11. **Das, Saikat**, Deepak Venugopal, and Sajjan Shiva. "A Holistic Approach for Detecting DDoS Attacks by Using Ensemble Unsupervised Machine Learning." In Future of Information and Communication Conference, pp. 721-738. Springer, Cham, 2020.

12. **Das, Saikat**, Ahmed M. Mahfouz, Deepak Venugopal, and Sajjan Shiva. "DDoS intrusion detection through machine learning ensemble." In 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 471-477. IEEE, 2019.

13. **Das, Saikat**, Ahmed M. Mahfouz, and Sajjan Shiva. "A Stealth Migration Approach to Moving Target Defense in Cloud Computing." In Proceedings of the Future Technologies Conference, pp. 394-410. Springer, Cham, 2019.

14. **Das, Saikat**, and Sajjan Shiva, "CoRuM: collaborative runtime monitor framework for application security.", 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), IEEE, 2018.

15. Mesbah-Ul-Awal, Md, Muhammad Sheikh Sadi, and **Saikat Das**. "Component Criticality Analysis: An Efficient Approach towards Minimizing the Risks of System Software Failure." Physical Science International Journal (2014): 231-245.

16. Mesbah-Ul-Awal, Md, and **Saikat Das**. "Component Criticality Approach towards Minimizing the Risks of System Failure." 2013 Third International Conference on Advanced Computing and Communication Technologies (ACCT). IEEE, 2013.

## Technical Skills

- **Languages:** Python, PHP, SQL, Java, Ruby on Rails, Perl, MATLAB, JavaScript, C++, C# and C.
- **Machine learning Tools:** scikit-learn, Keras, TensorFlow, nltk, pandas, numpy, etc.
- **Technologies, Operating Systems and Servers:** MySQL, PostgreSQL, SQLite, NoSQL, Oracle 11g, Hadoop, Spark, Weka, Git, SVN, Slack, Jira, Windows, Linux Ubuntu, MacOS, Amazon EC2, Eclipse, Visual Studio, Jupyter notebook, etc.

## Academic Projects

**DDoS Explainer and Feature Selector (IMLFS)**

- Implemented a feature selection process using Interpretable Machine Learning explainer model.
- The test F1-score of IMLFS (0.940), which is 5.60% higher than a classical feature selection.

**SCADA, IDS, and IPS in Smart Grid**

- Designed SCADA and developed IDS & IPS in a simulated smart grid.
- Detected and prevented DDoS, Packet Drop and Bad Data Injection attacks in Simulink.

**Ensemble Feature Selector**

- Implemented a framework that ensembles feature selection methods using majority voting technique to select best features for DDoS attack detection in scikit-learn, Python

**Ensemble Machine Learning (ML) Frameworks**

- Developed ensemble frameworks with supervised and unsupervised ML models.
- Detected and analyzed DDoS attacks using NSL-KDD, CICIDS2017, and UNSW-15 datasets.
- Implemented ensemble feature selection which increases the accuracy of 5% than LASSO.

**NLP based IDS**

- Implemented Doc2Vec and SVM model to detect anomalous traffic using HTTP CSIC 2010 dataset.
- Improved detection accuracy compared to existing work.

**Stealth Migration Protocol**

- Designed a stealth migration protocol to migrate VM in cloud using OpenStack.
- Prevented man-in-the middle attacks during VM migration.

**Evolutionary Approach in IDS:**

- To improve rule-based IDS and detect SQL injection attacks, designed a GA based IDS in Python with Random Forests and SVM models using HTTP CSIC 2010 dataset.

**Collaborative Runtime Monitor**

- Developed a collaborative runtime monitor with several agents to detect and prevent attackers, and implemented honeypot & backup server to improve system's security  resiliency in PHP.

**Student Management Portal**

- Designed and developed web-based management portal in Ruby on Rails for students to create forums, groups, self-configuring to-do lists, etc. (study through communication)

**Secure File Management System:**

- Implemented a web-based secure file mgmt. system to manage (i.e.; CRUD operations) files securely with a key-based file encryption/decryption using RSA cryptography in PHP.

**Websites and Applications**

- During undergraduate studies, several websites are designed and developed as course projects like student course registration, university grading system, online quizzing, etc. in PHP.
- Implemented mobile application in Java for medicine salesman to fetch inventory, order items, etc.

# Major Courses

- **Graduate Level**: Network Security, Cryptography, Cloud Computing, Evolutionary Computing, Real Time Operating System, Machine Learning, Data Science, Information Retrieval, Natural Language Processing, Parallel Computing, Distributed System, Foundation of Computing, Problem Solving/ Algorithm, Software Engineering, etc.

- **Undergraduate Level**: Operating Systems, Database Systems, Algorithm, Programming Language, Computer Architecture, Data Structure, Computer Networks, Computer Graphics, Artificial Intelligence, Discrete Mathematics, Graph Theory, Digital Logic Design, Microprocessor, Digital System Design, Peripheral Interface, etc.

# Program and Course Development

- Cyber Defense Program at Southwest Tennessee Community College, Memphis, TN

- Courses
  - Computer Applications (INFS 1010)
  - Principles of Information Assurance (CITC 1351)
  - Network Security (CITC 2326)
  - Digital Forensics (CITC 2352)
  - Tactical Perimeter Defense (CITC 2353)

# Teaching Experience

**INFS 1010 Computer Applications - Lecturer**

Fall 2018 and Spring 2019 (Southwest TN Community College)
This course is designed to enable students to utilize the current Windows operating system, file and folder management, along with Office applications in a business environment. The course will use the following Office applications: word processing, spreadsheet, database, and presentation software. In addition, students will learn essential computer concepts and terminology needed to succeed in today's information society. Keyboarding skills are required by the student to work in a timely fashion.

**CITC 1351 Principles of Information Assurance - Lecturer**

Fall 2018 and Spring 2019 (Southwest TN Community College)
A beginning course in information assurance which examines the fundamentals of information assurance. The course will introduce topics such as the need for security, risk management, security technology, cryptography, and physical security. Also covered are legal/ethical issues and security policies.

**CITC 2326 Network Security - Lecturer**

Fall 2018 and Spring 2019 (Southwest TN Community College)
This course is designed to give students a fundamental understanding of computer and network security. It will introduce students to a wide variety of concepts related to network security. This course will cover the objectives for the current CompTIASecurity+ Certification.

**CITC 2352 Digital Forensics - Lecturer**

Fall 2018 and Spring 2019 (Southwest TN Community College)
This course is designed to give students a basic understanding of computer forensics and investigations. This course will introduce students to computing investigations by preparing them to acquire, examine and summarize digital evidence.

**CITC 2353 Tactical Perimeter Defense - Lecturer**

Spring 2019 (Southwest TN Community College)
An examination of how software and hardware can be used to provide a perimeter of defense in protecting resources, and how security is addressed in both wireless and wired networks. Topics include the use of tools such as wireless access points, proxy servers, VPNs, auditing, intrusion detection systems and firewalls.

**COMP 3410 - Computer Organization, Design and Architecture - Teaching Assistant**

Spring 2018,2020,2021 and Fall 2017, 2020 (University of Memphis)
Basic concepts in assembly language programming, including logic, comparing and branching, interrupts, macros, procedures, arrays, program design, testing, debugging, loading, and linking; combinational, arithmetic and logical circuits ALU; memory circuits, latches, flip-flops, registers; computer structure; fetch-execute cycles, clocks and timing; microprogramming and microarchitecture; data path, timing, sequencing; cache memory organization; RISC architectures.

**COMP 7720 - Artificial Intelligence - Teaching Assistant**

Fall 2019 (University of Memphis)
Central issues of artificial intelligence, including game playing, planning, machine learning, commonsense reasoning, perception and action; implementations in LISP.

**COMP 6040 - Programming Languages - Teaching Assistant**

Fall 2015, Spring 2016 (University of Memphis)
Comparative features, syntax and applicability of high-level programming languages such as FORTRAN, PASCAL, LISP, Scheme, ADA, C, C++, JAVA, PHP, JavaScript, Perl, Prolog, FORTH; data types, data structures, dataflow; procedures, recursion, runtime environment, string manipulation, list processing, array processing, documentation, programming style

**COMP 8120 - Cryptography and Data Security - Teaching Assistant**

Spring 2016 (University of Memphis)
This course is an introduction to the basic concepts and mechanisms of applied cryptography and data security. It will cover both cryptographic primitives (symmetric encryption, public encryption, MACs, Digital Signatures, Authenticated Encryption, etc.) to cope with the data confidentiality and data integrity. It also emphasizes on how to apply and implement cryptography in practice

### CSC 210 C++ Introduction for Programmers - Teaching Assistant

Fall 2014 (South Dakota School of Mines and Technology)
Learn to transition from Java, Python or other programming languages to C++. Explore the differences in memory management, classes, and pointers to become an effective C++ programmer. Learn to work with the Standard Template Library to create concise, efficient, and readable programs in C++.

## Training Programs

### National Cyber Watch Center

Prince George's Community College, Largo, MD, USA June 12-14, 2019

**Skill Learned:** As a professional development training, it provided the guidelines to enhance the Community College Cyber Defense program and to encourage the high school students studying in cyber security, as well as to develop a relationship between industry and college graduates.

### Problem Solving & Language Adaptability Training (As a trainer)

Samsung Research and Development Institute, Dhaka, Bangladesh March - May 2014

**Skill Learned:** Conducted a training program for the fresh software engineers inside Samsung Research & Development Center, Bangladesh, to train them how to solve the problems, showed different strategies on problem solving skills, and introduced different programming language skills like java, C++, and web programming.

### Cisco Network Academy Program (CNAP)

Khulna University of Engineering & Technology, Khulna, Bangladesh May 2010- April 2011

**Skill Learned:** Preparation for CISCO certification exam that included the following topics: Network Fundamentals, Routing Protocols & Concepts, LAN Switching & Wireless, and Accessing the WAN.

## Voluntary Activities

- **Reviewer**, IEEE Open Journal of the Communications Society 2021
- **Reviewer**, IEEE International Conference on Communications, Network, and Satellite 2021, 2020
- **Reviewer**, Elsevier Journal of Information Security and Applications 2021, 2020
- **Reviewer**, Elsevier International Journal of Electrical Power & Energy Systems 2021
- **Reviewer**, The 4th International Conference on Mechanical, Electric and Industrial Engr 2021
- **Reviewer**, Elsevier Books 2020
- **Reviewer**, Elsevier Computer & Security 2020
- **Reviewer**, IEEE International Conference on Industry 4.0, AI and Communications Tech. 2020
- **Reviewer**, IEEE International Conference on Signals and Systems, ICSigSys 2019
- **Event Supervisor**, Codebusters, Science Olympiad, Memphis, TN 2nd March 2019
- **Executive Officer**, Bangladesh Student Association at UofM, Memphis, TN July-December 2016
- **Volunteer**, Cyber Security Summit, CfIA, University of Memphis 16th October 2015