# CURRICULUM VITAE

**Name: Dr. Shaik Shakeel Ahamad**
**Majmaah University,**

**Kingdom of Saudi Arabia**

**Mobile No: +966583198711**

**E mail:ahamadss786@gmail.com & s.ahamad@mu.edu.sa**

## Areas of Interest

- Security in Mobile Payments (Remote and Proximity), PKI, Wireless PKI, NFC Security Information security, Mobile Payment and Commerce Protocols, cloud computing, Mobile Cloud Computing, Mobile Ad hoc Networks, Multi-hop Cellular Networks, 5G / future (beyond 4G) smartphone, wireless network technologies & Cyber Security (computer forensics, network forensics, forensic data analysis and mobile device forensics).

## Education

**Ph.D (Computer Science) full-time** from **University of Hyderabad (UoH) (a Central University), India & IDRBT (a subsidiary of Reserve Bank of India)** under the supervision of **Prof.V.N.Sastry** (Prof. in IDRBT & Executive Secretary of **Mobile Payment Forum of India (MPFI))** & **Prof. Siba Kumar Udgata (Prof. in UoH) & Director of CMSD.**

**Thesis Title:** "Design of Protocols for Secure Mobile Payments and their Formal Verification" **(Awarded on 3rd Feb 2014)**

## Employment History

**August 2015- Till date**

Working as an Assistant Professor in CCIS at Majmaah University, Majmaah, Kingdom of Saudi Arabia.

**April 2014 – August 2015**

Worked as a Professor (Now on lien) in CSE at KL University, Guntur, Andhra Pradesh, India (Full Time) & Head of Computer & Network Security Research Group.

**October 2013 – March 2014**

a) Worked as an Associate Professor in Anwarul Uloom College for Computer Science, Hyderabad, AP. (Full Time)
b) PKI Trainer & Consultant (Part Time) at E2 Labs, Hyderabad, India

**June 2013- October 2013**

a) Worked as an Associate Professor in CSE and Director of Research & Development at K.G.Reddy College of Engineering & Technology, Moinabad, Hyderabad, AP. (Full Time)

b) PKI Trainer & Consultant (Part Time) at E2 Labs, Hyderabad, India

**Nov 1999 - August 2008**

Worked as an Assistant Professor, Anwarul Uloom College for Computer Studies (MCA College), Affiliated to Osmania University, New Mallepally, and Hyderabad, India.

**Positions held**

a) Member, Academic Council

b) Member, Board of Studies CSE

c) Head, Computer & Network Security Research Group

d) Chairman, Students Research & Development Activities

e) In charge of Heterogeneous Mobile Network lab (FIST Scheme)

## Main Job Responsibilities as a Researcher (while pursuing Ph.D (Computer Science))

a) Designing and implementing Secure Mobile Payment protocols which ensure all the security properties (such as Authentication, Confidentiality, Integrity and Non Repudiation) which consume fewer client resources (i.e. to reduce communication and computational cost).

b) Designing and implementing Secure Payment protocols which ensure all the security properties (such as Authentication, Confidentiality, Integrity and Non Repudiation) in the realm of Mobile Ad hoc Networks.

c) Train researchers, M.Tech students and IT officers from Banks and Financial Institutions to practically understand the current Mobile Banking Security Models, frameworks, best practices and evolving challenges.

d) Provide solutions by analyzing the emerging attacks on mobile phones and frauds happening through mobile banking.

e) Provide consultancy to Banks & Financial Institutions in policy framework, technical guidance, testing, evaluation, etc.

f) Building inter-disciplinary research activities (e.g., Secure Mobile Payments in Mobile Cloud Computing)

g) Real Time Implementation and Deployment of our proposed protocols using EJBCA, J2ME (WTK), Java Card 3.0.2, Java Card OpenPlatform (JCOP), Nokia NFC 6131 SDK, Nokia NFC 6212 SDK, AVISPA (Automated Validation of Internet Security Protocols and Applications), SPAN v1.6 and Scyther 1.0-rc1

# TECHNICAL SKILLS

- **Operating Systems:** Microsoft Windows vista/XP/7, Experience with Red Hat Linux and Fedora Linux
- **Programming Languages:** C/C++, Java 1.6, Java Cryptographic Extensions (JCE), Design Patterns, UNIX Shell Programming, Socket Programming Remote Procedure Calls
- **Mobile Development Platforms:** J2ME (WTK), Java Card 3.0.2, Java Card OpenPlatform (JCOP)

- **Software Development Kit (SDK's):** Nokia NFC 6131 SDK, Nokia NFC 6212 SDK, Android SDK

- **Integrated Development Environment (IDE):** Net beans 6.9 & 6.8, Eclipse Helios 3.6

- **Client Server Data Transfer:** XML, XML Schema

- **Mobile OS Framework Programming**: Android NFC & Android Bluetooth

- **Implementation of PKI:** JCE as well as OpenSSL and Java Keytool use, EJBCA, CSRTOOL, CertForge, OpenCA and XCA (Using these Tools I have created Key pairs, Generated X.509 Certificates, Signed X.509 Certificates, Managed CMP (Certificate Management Protocol), Certificate Revocations using CRL and OCSP.

- **Implemented** "Secure Mobile Payments(Remote and Proximity) Framework based on Wireless PKI" using J2ME, Java Card, CAT Loader, Nokia 6131, 6212 SDK's, EJBCA, CSRTOOL, CertForge, OpenCA and XCA

- **XML Implementation/Technologies:** Experience with authentication, authorization, cryptography, electronic commerce, Mobile Commerce, PKI, Wireless/Mobile PKI, SPKI, smartcards, Single Sign-On (SSO), Implemented XML security standards such as XML digital signature, XML encryption, XML canonicalization, HTML5, XML, XSLT, JSP, J2EE, Web Services and REST
- **Specifications:** Good Understanding and real-time implementation of Global System for Mobile Communications (GSM) including GSM evolved radio access technologies (e.g. General Packet Radio Service (GPRS) and Enhanced Data Rates for GSM Evolution (EDGE)), IP Multimedia Subsystem (IMS), NFC (NFC Forum), Global Platform specifications , PCI DSS (Payment Card Industry Data Security Standard)
- **Formal Verification Tools:** AVISPA (Automated Validation of Internet Security Protocols and Applications), SPAN v1.6 and Scyther 1.0-rc1.

## Patents

1) Shaik Shakeel Ahamad., (October, 2014) Indian Patent Application No. 5240/CHE/2014

   **Title of the filed patent:** System and Method for Ensuring End to End Security in Mobile Commerce

2) Shaik Shakeel Ahamad., (Feb, 2015) Indian Patent Application No.

   **Title of the filed patent:** Method and System using Signcryption Mechanism to provide secure transactions

## Sponsored Projects Applied/Submitted

1) **Title of the Project Applied:** Design and Development of Secure Mobile Payment Framework based on Mobile Public Key Infrastructure (MPKI) and Elliptic Curve Cryptography Algorithm

   **Name of the Sponsoring Agency:** Department of Electronics and Information Technology, Ministry of Communications and IT

   **Total Budget of the Applied Project:** 47, 23,443 INR

   **Date:** 24th October 2014

   **Chief Investigator:** Dr. Shaik Shakeel Ahamad, Dept of CSE, KL University, Guntur, A.P

   **Co-Investigator:** Dr. K. Thirupathi Rao, Dept of CSE, KL University, Guntur, A.P

2) **Title of the Project Applied:** DESIGN AND DEVELOPMENT OF SECURE MOBILE GOVERNANCE FRAMEWORK BASED ON MOBILE CLOUD COMPUTING FOR INDIA

   **Name of the Sponsoring Agency:** Department of Science & Technology, New Delhi

   **Total Budget of the Applied Project: 51, 87,443 INR**

   **Date:** 17th January 2015

   **Chief Investigator:** Dr. Shaik Shakeel Ahamad, Department of CSE, KL University, Guntur, A.P

   **Co-Investigator:** Dr. V. Krishna Reddy, Department of CSE, KL University, Guntur, A.P

# PUBLICATIONS IN JOURNALS

1. Shaik Shakeel Ahamad, Udgata, S.K. and Sastry, V.N. (2012). A new mobile payment system with formal verification. *International Journal of Internet Technology and Secured Transactions*, 4(1), 71–103. (Inderscience Publications) **(Indexed by ACM Digital Library, Scopus, Scirus), ISSN: 1748-569X, EISSN: 1748-5703 & doi: 10.1504/IJITST.2012.045153**

2. Shaik Shakeel Ahamad., Sastry, V.N. and Udgata, S.K. (2012). Secure and Optimized Mobile based Merchant Payment Protocol using Signcryption. *International Journal of Information Security and Privacy*, 6(2), 64-94. (IGI Global Publications) **(Indexed by ACM Digital Library, DBLP, Scopus), ISSN: 1930-1650, EISSN: 1930-1669 & doi: 10.4018/jisp.2012040105**

3. Shaik Shakeel Ahamad., Sastry, V.N. and Udgata, S.K. (2012). A Secure Mobile Wallet Framework with Formal Verification. *International Journal of Advanced Pervasive and Ubiquitous Computing (IJAPUC)*, 4(2), 1-15. (IGI Global Publications) **(Indexed by ACM Digital Library, DBLP), ISSN: 1937-965X, EISSN: 1937-9668 & doi: 10.4018/japuc.2012040101**

4. Shaik Shakeel Ahamad., V.N.Sastry & Siba K.Udgata (2013). A Secure Mobile Payment Framework in MANET Environment. *International Journal of E-Business Research (IJEBR),* 9(1), 54-84. (IGI Global Publications) **(Indexed by ACM Digital Library, DBLP and Scopus), ISSN: 1548-1131, EISSN: 1548-114X & DOI: 10.4018/IJEBR**

5. Shaik Shakeel Ahamad, V. N. Sastry, Siba K. Udgata: A Secure and Optimized Proximity Mobile Payment Framework with Formal Verification. *International Journal of E-Services and Mobile Applications (IJESMA)* 6(1): 66-92 (2014) (IGI Global Publications) **(Indexed by DBLP, Scopus), DOI: 10.4018/ijesma.2014010104**, **ISSN: 1941-627X & EISSN: 1941-6288**

6. Shaik Shakeel Ahamad, V. N. Sastry, Siba K. Udgata: Secure mobile payment framework based on UICC with formal verification. *International Journal of Computational Science and Engineering* (IJCSE). 9(4): 355-370 (2014) **(Indexed by ACM Digital Library, DBLP, Scopus), ISSN online: 1742-7193, ISSN print: 1742-7185 & DOI: 10.1504/IJCSE.2014.060718**

# PUBLICATIONS IN CONFERENCES

1. Shaik Shakeel Ahamad, V. N. Sastry, Siba K. Udgata: A secure and optimized mobile payment framework with formal verification. In *Proceedings of First International Conference on Security of Internet of Things (SECURIT 2012), Amrita Vishwa Vidyapeetham*, (pp. 27-35), August 16-19, 2012. **(Indexed by DBLP, ACM Digital Library), ISBN 978-1-4503-1822-8**

2. Shaik Shakeel Ahamad, Sastry, V.N.; Udgata, Siba K. (2012). Enhanced Mobile SET Protocol with Formal Verification. In *Procedings of Third International Conference on Computer and Communication Technology (ICCCT)* (pp.288-293). **(Indexed by IEEE Digital Library, ACM Digital Library), ISBN: 978-0-7695-4872-2 & doi:10.1109/ICCCT.2012.65**

3. Shaik Shakeel Ahamad, Sastry, V.N.; Madhusoodhnan Nair (2013). A Biometric based Secure Mobile Payment Framework. Fourth *International Conference on Computer and Communication Technology (ICCCT),* Date of Conference: 20-22 Sept. 2013, Page(s):
   239 – 246, **Print ISBN: 978-1-4799-1569-9, INSPEC Accession Number: 14130815**,
   Allahabad, **(Indexed by IEEE Digital Library, ACM Digital Library)**

4. Shaik Shakeel Ahamad, Sastry, V.N.; Siba K. Udgata; Madhusoodhnan Nair (2013). A Secure and Reliable Mobile Banking Framework. In ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India- Vol II. Advances in Intelligent Systems and Computing Volume 249, 2014, pp 741-748. **(Indexed by Springer, DBLP and Scopus) DOI: 10.1007/978-3-319-03095-1_80, Print ISBN: 978-3-319-03094-4, Online ISBN: 978-3-319-03095-1**

5. Shaik Shakeel Ahamad, Siba K. Udgata; Madhusoodhnan Nair (2013). A Secure Lightweight and Scalable Mobile Payment Framework. FICTA 2013: 545-553, at Bhuneshwar, India. **ISBN: 978-3-319-02930-6 (Indexed by Springer, DBLP and Scopus)**

6. Pavan, Shaik Shakeel Ahamad, V.N.Sastry & Siba K.Udgata. A Secure Mobile Payment Framework using WPKI for India. In *Proceedings of International Workshop on Information Security Applications*, Jeju Islands, South Korea**,** August 22-24, 2011

7. Shaik Shakeel Ahamad., and V.N.Sastry. Importance and Issues of Implementing Public Key Infrastructure for Mobile Payments. *Presented at Seventh Meeting of Mobile Payment Forum of India (MPFI) held on April 17, 2010 at IDRBT,* Hyderabad http://www.mpf.org.in/meetings.html

8. Shaik Shakeel Ahamad and V.N.Sastry, "Basics of Structured Financial Messaging System (SFMS) Standard for Mobile Payments in India" **presented at Second MPFI meeting conducted on 16th Feb 2008 at IIT Madras, Chennai** http://www.mpf.org.in/pdf/Basics%20of%20SFMS%20Standards.pdf.

## Books

Shaik Shakeel Ahamad, Network Security, Sure Publications for MCA Final Year Second Semester of Osmania University, Hyderabad

## Courses Taught at P.G. Level

Mobile Computing, Computer Networks, Network Programming, Network Security, Mobile Commerce, E-Commerce, Mobile Ad hoc Networks

## Lectures and Talks Given

- Took ten sessions of "Network Programming and Web Services" subject lab for the batches 2007-2008 & 2008-2009 of M.Tech (IT) First Year at IDRBT
- Took a session on the "Network Programming using C and Java" for Scientists of DRDO New Delhi from 15th -17th June 2011
- Took a session on the "Security issues in Mobile Payments" in Executive Development Programme (EDP) on "Wireless Technologies & Mobile Payments" conducted at IDRBT on 8th Dec 2009.

  Took a session on "Authentication in the Banking Paradigm" in Executive Development Programme (EDP) on "Mobile Banking" conducted at IDRBT from 15th -16th Feb 2010.
- Took a session on "Security issues in Mobile Payments" in Executive Development Programme (EDP) on "Mobile Banking" conducted at IDRBT from 15th to 16th Feb 2010.
- Talk given on "Wireless PKI for Mobile Payments" at Seventh Meeting of Mobile Payment Forum of India (MPFI) held on April 17, 2010 at IDRBT, Hyderabad http://www.mpf.org.in/meetings.html
- Took a session on "Security issues in Mobile Payments" in Executive Development Programme (EDP) on "Mobile Banking" conducted at IDRBT from 17th to 18th June 2010.
- Took a session on the "Proximity Mobile Payments Using NFC, RFID, Barcodes and Bluetooth" in Executive Development Programme (EDP) on "Wireless Technologies & Mobile Payments" conducted at IDRBT on 16th Feb 2011.
- Took a session on the "Wireless Public Key Infrastructure (WPKI) Mobile Payments" in Executive Development Programme (EDP) on "Wireless Technologies & Mobile Payments" conducted at IDRBT on 17th Feb 2011.
- Took a session on the "J2ME & WAP" in Executive Development Programme (EDP) on "Wireless Technologies & Mobile Payments" conducted at IDRBT on 17th Feb 2011.
- Took two sessions on "Socket Programming using C" for SAG Scientists of DRDO, New Delhi from 15th to 17th June 2011.
- Took a session on the "Wireless PKI for Mobile Payments" in Executive Development Programme (EDP) on "Mobile Banking" conducted at IDRBT on june 30th 2011.

# CONFERENCES & PROGRAMS ATTENDED

- Attended the First meeting of the Mobile Payment Forum of India conducted at IDRBT Hyderabad on 15th Sept 2007.
- Attended a workshop on "Free/Open source software" conducted by IEEE in association with Department of Computer & Information Sciences, University of Hyderabad at University of Hyderabad on 27th October 2007.
- Attended Executive Development Program (EDP) on "Networking Technologies for Canara Bank" from 10th to 14th December 2007 conducted at IDRBT Hyderabad.
- Attended Fourth "International Conference on Distributed Computing & Internet Technology (ICDCIT)-2007" from 17th to 20th December 2007 at Bangalore. Jointly organized by KIIT Bhubaneshwar & UNU-IIST Macauo.
- Attended a workshop on "MANETS: Issues and Challenges" held from 10th to 11th January 2008 at Osmania University, Hyderabad.
- Attended Executive Development Program (EDP) on "Mobile Banking" Conducted at IDRBT from 12th & 13th May 2008.
- Attended talks on cryptography given by Prof.BIMAL ROY (ISI, Kolkata) at Dr.C.R.Rao Institute for Advanced Studies on 15th October 2009.
- Attended Executive Development Program (EDP) on "Wireless Technologies & Mobile Payments" conducted at IDRBT from 7th to 9th Dec 2009.
- Attended a workshop "International School on Logic and its Applications (ISLA) 2010" conducted by Association for Logic in India, held at the University of Hyderabad, Gachibowli, India, from **18th –29th January 2010.**
- Attended Executive Development Program (EDP) on "Mobile Banking" conducted at IDRBT from 15th to 16th Feb 2010.
- Attended Seventh Meeting of MPFI held on April 17, 2010 at IDRBT, Hyderabad http://www.mpf.org.in/meetings.html http://www.mpf.org.in/meetings.html%23w9
- Attended Executive Development Program (EDP) on "Financial Inclusion" conducted at IDRBT from 28th to 30th April 2010.
- Attended Executive Development Program (EDP) on "Mobile Banking" conducted at IDRBT from 17th to 18th June 2010.
- **Attended 10 days training program on "Computer Forensics" conducted by "Encase USA" in CCIS, Majmaah University, KSA from 11th October 2015 to 20th October 2015 (Speaker was Charles Gigla, Vice President, Encase USA).**

## AWARDS & RECOGNITIONS

1. **Actively involved in the establishment of the Mobile Banking Security Lab (MBSL) at IDRBT as a team leader which was inaugurated by Hon. RBI Governor Dr. Subbarao on 3rd August 2012. Developed prototypes of many Secure Mobile Payment Protocols which ensured end to end security in MBSL.** **http://www.idrbt.ac.in/PDFs/MBSL_Brochure_final.pdf**
2. **Reviewer of**

   **Journals:**

   a) **Computers & Electrical Engineering (Elsevier) (five year Impact Factor: 1.09)**

   b) **Digital Investigation Journal (Elsevier) (five year Impact Factor: 1.171)**

   c) Information Security Journal: A Global Perspective Journals **(Taylor & Francis publications)**

   d) International Journal of E-Services and Mobile Applications (IJESMA) **(IGI Global)**

   e) International Journal of Network Security

   **Conferences:**

   a) The International Conference of Digital Enterprise and Information Systems (DEIS 2011) conducted by London Metropolitan Business School, United Kingdom.

   b) ICCCT (2014) conducted by Osmania University, Hyderabad, India
3. **Program Chair for** ICCCT (2014) conducted by Osmania University, Hyderabad, India
4. **Co-Session chair for International Conference on Signal Processing And Communication Engineering Systems (SPACES 2015), conducted from 2nd to 3rd Jan 2015 at KL University.**
5. Stood Second in the Ph.D (Computer Science) entrance test and Interview conducted by University of Hyderabad in 2007
6. Received IDRBT Doctoral Fellowship for Five Years from Reserve Bank of India
7. Talk given on “Network Programming using C and Java” for Scientists of DRDO New Delhi from 15th -17th June 2011
8. Talk given on “Wireless PKI for Mobile Payments” at Seventh Meeting of Mobile Payment Forum of India (MPFI) held on April 17, 2010 at IDRBT, Hyderabad http://www.mpf.org.in/meetings.html

# RESEARCH GUIDANCE

| S.No | Name of the Scholar | University | Major Research Area | Specialization | Status |
|---|---|---|---|---|---|
| 1 | PMD Nagarjun | KL University | Computer Science and Engineering | Secure Proximity based Mobile Payment Frameworks | On going |
| 2 | Reshma Sujal Sonar | KL University | Computer Science and Engineering | Communication Security in Mobile Environment | On going |
| 3 | Bejjam Jyoshna | KL University | Computer Science and Engineering | Cloud Forensics | On going |
| 4 | Srinivasa Rao Kosiganti | KL University | Computer Science and Engineering | Cloud based Mobile Commerce | On going |
| 5 | Riaz Shaik | KL University | Computer Science and Engineering | Security issues in wireless sensor networks | On going |
| 6 | Vijay kumar mantri | KL University | Computer Science and Engineering | Secure Software Engineering | On going |
| 7 | Divya Tamma | KL University | Computer Science and Engineering | Secure Cloud Computing | On going |

# PERSONAL INFORMATION

Father's Name: John Ahamad (Retired Teacher Govt. Boys High School)

Mother's Name: Late Khudisiya Begum (Retired Principal Govt. Girls High School)

Gender: Male

Citizenship: Citizen of India.
Religion: Islam
Languages known: English, Telugu, Hindi and Urdu

**Current Address**

Majmaah

Kingdom of Saudi Arabia

Mobile No: +966583198711

**Permanent Residential Address:**

Dr. Shaik Shakeel Ahamad,

H.No: 39-5-7A,

Mouli Saheb Street, Lane opposite to Dars-Gaha-Islamia,

Lane opposite to Cinepolis, Labbipet,

Vijayawada-520010

Mob No: +91-9949235872,

Email: ahamadss786@gmail.com;

ssahamad786@kluniversity.in

# REFERENCES

- **Prof. V.N.Sastry (Professor)**

  Institute for Development & Research in Banking Technology (IDRBT), Road No 1,

  Castle Hills, Masab Tank, Hyderabad-500057, India

  E-Mail: vnsastry@idrbt.ac.in
  Phone: +91-040-23534981 to 84, extn.2031
  URL: http://www.idrbt.ac.in

- **Prof. Siba Kumar Udgata (Professor)**

  School of Computer and Information Sciences,

  University of Hyderabad, Gachibowli, Hyderabad, India

  Email: udgatacs@uohyd.ernet.in

  Phone: +91-40 23134119 (Work)

- **Prof.C.Raghavendra Rao (Professor)**

  School of Computer and Information Sciences,

  University of Hyderabad, Gachibowli, Hyderabad, India

  Email:crrsm@uohyd.ernet.in

  Phone: +91-040-23010780

## REAL TIME PROJECTS IMPLEMENTED AT IDRBT (ESTABLISHED BY RESERVE BANK OF INDIA)

These are the projects which are implemented as part of my Ph.D. (Computer Science) program at MBSL (Mobile Banking Security Lab) at IDRBT which was inaugurated by RBI Governor Dr.Subbarao

**Project 1:**

**Project Title:** Design and Development of WPKI for Secure Mobile Payments (using RSA)
**Project team size:** 6 Members
**My Role:** Project Leader
**Duration:** Jan 2009 to Dec 2010
**Gist of the project:**

This project was implemented using J2ME (WTK) for the client side, using EJBCA for the entire WPKI ecosystem, Issuer; Acquirer is implemented using Tomcat and Weblogic Server. The Integrated Development Environment (IDE) used is Net beans 6.9 & 6.8.

**Project 2:**

**Project Title:** Design and Development of WPKI for Secure Mobile Payments (using ECDSA)
**Project team size:** 6 Members
**My Role:** Project Leader
**Duration:** Jan 2009 to Dec 2010
**Gist of the project:**

This project was implemented using J2ME (WTK) and Bluetooth JSR82 API package. The JSR82 API has capability to provide all three kinds of communications: Obex, L2CAP, or RFCOMM. The communication between Bluetooth enabled mobile phone and Bluetooth enabled POS is Bluetooth. EJBCA is used for the entire WPKI ecosystem, Issuer; Acquirer is implemented using Tomcat and Weblogic Server. Using these Tools I have created Key pairs, Generated X.509 Certificates, Signed X.509 Certificates, Managed CMP (Certificate Management Protocol), Certificate Revocations by CRL and OCSP

**Project 3:**

**Project Title:** Proximity (using Bluetooth and NFC) Mobile Payments using WPKI in the memory of Mobile Phone
**Project team size:** 6 Members
**My Role:** Project Leader
**Duration:** Jan 2011 to May 2012 (15 Months)
**Gist of the project:**

This project was implemented using Nokia 6131, 6212 SDK's the communication between NFC enabled mobile phone and NFC enabled POS is NFC. EJBCA is used for the entire WPKI ecosystem, Issuer; Acquirer is implemented using Tomcat and Weblogic Server. Using these Tools I have created Key pairs, Generated X.509 Certificates, Signed X.509 Certificates, Managed CMP (Certificate Management Protocol), Certificate Revocations by CRL and OCSP

**Project 4:**
**Project Title:** Proximity (using Bluetooth and NFC) Mobile Payments using WPKI in UICC (Universal Integrated Circuit Card)
**Project team size:** 6 Members

**My Role:** Project Leader
**Duration:** Jan 2011 to May 2012 (15 Months)
**Gist of the project:**

This project was implemented using Javacard 3.1, CAT Loader. The JSR82 API has capability to provide all three kinds of communications: Obex, L2CAP, or RFCOMM. The communication between Bluetooth enabled mobile phone and Bluetooth enabled POS is Bluetooth. The difference between this implementation and its counterpart (i.e. in the memory of mobile phone) is that credentials of the client are generated and stored in the SE (SIM/UICC). EJBCA is used for the entire WPKI ecosystem, Issuer; Acquirer is implemented using Tomcat and Weblogic Server. Using these Tools I have created Key pairs, Generated X.509 Certificates, Signed X.509 Certificates, Managed CMP (Certificate Management Protocol), Certificate Revocations by CRL and OCSP

**Project 5:**
**Project Title:** Secure Mobile Payments with open SSL and Wireless PKI certificate
Validation process
**Project team size:** 6 Members
**My Role:** Project Leader
**Duration:** Jan 2011 to May 2012 (15 Months)
**Gist of the project:**

This project was implemented using Javacard 3.1, CAT Loader and Bluetooth JSR82 API package. The difference between this implementation and its counterpart (i.e. in the memory of mobile phone) is that credentials of the client are generated and stored in the SE (SIM/UICC). The JSR82 API has capability to provide all three kinds of communications: Obex, L2CAP, or RFCOMM. The communication between Bluetooth enabled mobile phone and Bluetooth enabled POS is Bluetooth. EJBCA is used for the entire WPKI ecosystem, Issuer; Acquirer is implemented using Tomcat and Weblogic Server. Using these Tools I have created Key pairs, Generated X.509 Certificates, Signed X.509 Certificates, Managed CMP (Certificate Management Protocol), Certificate Revocations by CRL and OCSP

**Project 6:**
**Project Title:** Mobile wallets with proximity payments using Near Field Communication (NFC)
**Project team size:** 6 Members
**My Role:** Project Leader
**Duration:** Jan 2011 to May 2012 (15 Months)

**Gist of the project:**

This project was implemented using Javacard 3.1, CAT Loader the communication between NFC enabled mobile phone and NFC enabled POS is NFC. The difference between this implementation and its counterpart (i.e. in the memory of mobile phone) is that credentials of the client are generated and stored in the SE (SIM/UICC). EJBCA is used for the entire WPKI ecosystem, Issuer; Acquirer is implemented using Tomcat and Weblogic Server. Using these Tools I have created Key pairs, Generated X.509 Certificates, Signed X.509 Certificates, Managed CMP (Certificate Management Protocol), Certificate Revocations by CRL and OCSP

# STATEMENT ON CONTRIBUTION TO RESEARCH

My Ph.D. Thesis is in the realm of Mobile Payments Security, Mobile Commerce Security and NFC Security. I have proposed and implemented secure mobile payment frameworks suitable for wireless environments which ensures reliable and end to end communication security (using TCP and TLS) and end to end security at Application layer for financial transactions. I have Implemented Wireless Public Key Infrastructure (WPKI) which ensures end to end security for Mobile Payments. I have used Formal methods (BAN logic, SVO logic, AVISPA, Proverif and Scyther Tools) for the verification of my proposed secure payment protocols. I have implemented Secure Mobile Payment frameworks and protocols (Remote and Proximity) based on Wireless PKI using J2ME (WTK), Java Card 3.0.2, Java Card OpenPlatform (JCOP), CAT Loader, Nokia 6131, 6212 SDK's, . I have very good knowledge in SATSA, Bouncy Castle, Spongy Castle, EJBCA, PKI implementation using Microsoft Windows 2003 & 2008, OpenCA, XCA, Cryptography, JCA / JCE. I have used BAN logic, AVISPA and Scyther tools in my research. I have very good Experience in writing Mobile Banking/Commerce/payments Research Proposals.

## Current Research

**Mobile commerce using mobile cloud computing:**

The explosive growth of the mobile applications and emerging concept of cloud computing has introduced a new potential technology for mobile services known as mobile cloud computing (MCC). MCC integrates the cloud computing into the mobile environment and overcomes obstacles related to the performance (e.g., battery life, storage, and bandwidth), environment (e.g., heterogeneity, scalability, and availability), and security (e.g., reliability and privacy) which are vital in mobile computing. Mobile applications are gaining increasing share in a global mobile market. Various mobile applications have taken the advantages of MCC one of them is Mobile commerce. Mobile commerce using 4G and MCC will revolutionize Mobile commerce, 3G provides higher mobile bandwidth and vivid user interface and MCC provides PKI which has the ability of data processing, plenty of data memory and security. But mobile commerce based on MCC throws many security challenges which need to be addressed for the success of mobile commerce based on MCC. Security is the main concern in MCC which includes confidentiality, authentication, integrity, non-repudiation and fraud detection. Fraud is an intentional deception accomplished to secure an unfair gain, and an intrusion which are any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. Several threats may compromise the service or the contract between users and providers. Despite the use of traditional security defense mechanisms, cybercrimes on cloud computing infrastructure may always occur. It is therefore crucial to implement forensics techniques to help investigate cybercrime when they do happen. Several challenges raises such as how to collect data, where and how to store metadata for each transaction, how to analyze log files, how to identify attacks on cloud infrastructure. So digital forensic computing should be used to overcome the greatest challenges faced in dealing with frauds for Mobile commerce based on MCC.

Following are the contributions made by my research to the body of knowledge.

a) End to end security is ensured internally (i.e. inside the MCC) and during the transit of data from client to MCC.
b) Mobile Cloud is implemented in the UICC (client side)
c) Our proposed mobile commerce framework based on MCC will be implemented in UICC (Universal Integrated Circuit Card) which is a Secure Element (a generic platform for smart card applications). It has been standardized by ETSI EP SCP (ETSI Project Smart Card Platform). The UICC can host a number of different applications, each defining and controlling its own application(s). The architecture of our proposed mobile commerce framework based on MCC has

three layers of security they are Physical Infrastructure layer security, Communication layer security and Application layer security. Physical Infrastructure layer security is about GSM and GPRS security which is vulnerable to many attacks. Secure and reliable end to end communication between UICC and Cloud Service Provider (CSP) is ensured using SSL/TLS and TCP at Communication layer. Security at the application layer is ensured using HTTPS and our proposed mobile payment protocol. Provisioning is the process of installing a payment application on a UICC. Personalization is the process of putting data specific to a client into the mobile payment application. This includes providing the necessary cryptographic material required by the UICC or application in order to allow installation or personalization. It is also responsible for providing a chain of trust between the CSP and UICC, including appropriate logging to assist in audit, repudiation and forensic.

d) Detects flaws in the design of security protocols
e) Ensures Privacy/Anonymity

# STATEMENT ON TEACHING & CURRICULUM DEVELOPMENT

I have always felt enthusiastic about sharing the knowledge that I have learned or discovered with others. The other major reason why I want to be a teacher is that, from elementary to graduate school, I was lucky enough to meet several great mentors. They have had profound influences on different perspectives of my study and even life. I am looking forward to this aspect of my academic career and passing on their influences to others.

**Classroom Teaching:**
I have been in continuous interaction with undergraduate and post graduate students (Computer Science) since 1999. I worked hard to make my teaching inspiring and encouraging. I used to use textbooks, PowerPoint Presentations for making my lectures interesting. Some of my students became so interested that they even asked for additional work. I also had a student who did poorly at the beginning but due to my extra efforts and encouragement on him he understood the materials better and gained confidence. By the end of the semester, he was one of the top students in the class. I felt extremely happy for him.

**Curriculum Development:**

I have 8 years of experience as a member of Academic Council, Member of Board of Studies, Head of Computer & Network Security Research Group and Chairman of Students Research & Development Activities. So I had the opportunity to develop curriculum for both under graduates and post graduates.

**Research Mentoring:**

I have had the opportunities to mentor undergraduates, Masters Students for their projects.  I have been the graduate mentor of several undergraduate students participating in research programs over the past three summers. I met with them daily to help them understand what research is, do research, and present their research results formally. As a mentor for other graduate students in our group, I discuss ideas with them, provide suggestions when they are unsure how to proceed with their work, encourage them to work with me, and lead discussions in research project meetings. These experiences have well prepared me for advising my own students as a faculty member. I believe that the most important thing in teaching is to inspire students. Even if uninspired students work hard and get high scores, they will forget their hard learned knowledge soon after the semester ends. In contrast, inspired students will not only learn in class, they will also learn outside the classroom, from each other, and even after they graduate.  I also believe that teaching a student to become an independent thinker is very important. Even though I had many experiences in teaching and mentoring, I still have a lot to learn to achieve my developed teaching philosophy. I learned how to teach large size classes, teach classes of students with a mixture of backgrounds, and to achieve balance between teaching and research, etc, via a series of seminars provided by several well established teachers from several universities and webinars.

**Teaching Interests:**

I have a wide range of teaching interests. I can teach any undergraduate class and post graduate class in computer science. I look forward to giving back the knowledge I acquired through the years of my study, especially the topics related to Computer Networks, Mobile Computing, Network Security, Mobile Commerce, Java, Network Programming subjects.

# STATEMENT OF SERVICE PHILOSOPHY

Statement of Service Philosophy In my opinion, service is an opportunity to build robust relationships and partnerships – both within the department and between the department and the university and community. Service is a vehicle for collaboration, learning, knowledge sharing and creativity. I strongly believe that my commitment and willingness for service were established and developed due to my cultural background and through my extensive experience in research and academics. In that respect, service comes natural within my personality – especially when it comes to introducing initiatives, leading change and projects and collaborating within teams. I believe that any committee should be focused on achieving incremental targets that lead to its goal. Moreover, committees or teams should be viewed as vicinities for building networks and increasing personal development and exposure.

**Departmental service**: My previous departmental formal service was mostly focused on developing courses, curriculums & on improving research. Also, I was active in representing my department at conferences and advising students on their academic, career & research advancements. Additionally, I always made myself available to contribute to the work of other committees, especially when the help request falls within my area of expertise or when the committee is overloaded with work. I believe that the key attributes for successful service are willingness to help, share knowledge, collaborate and be involved with collective concerns and institutional development. Departmental service is integrated within my everyday work, so I do not consider it as an independent pillar when it comes to my personal performance. Although teaching is not usually considered under service, I believe that assisting others within the department to accommodate their teaching load with their personal and professional lives is a major service aspect. I always made myself available to substitute tutors, especially in cases of emergency and strong personal commitments. Such help provides the team with flexibility and, most importantly, increases cohesion and trust among the department members.

**University service**: I always looked at the university service as an opportunity to build cross-sectional networks and increase the department visibility. It is a great area where we can raise our voice for pressing needs and wants. Moreover, it increases the strength of the organizational culture and raises appreciation of other disciplines and units.

**Community service**: I strongly believe that one of the main roles of academics is to have an impact on their communities – especially when the community initiatives fall within my area of expertise. Partnerships with schools, colleges, other universities, governmental bodies/agencies and community organizations and influential individuals, help in strengthening the community, increasing the university visibility and elevating intrinsic rewards of academics.

**Professional service**: Another important area of academic impact is contributing to the professional community. I have been an active member of several professional organizations such as the CSI, IEEE. Professional organizations provide the opportunity to present your work, get feedback, interact with other academics and professionals, share knowledge and – most importantly – exert an effort to better the profession and foster creativity. To conclude, service should be looked at holistically – taking into account its various facets: departmental, organizational, communal and professional. It allows academics to impact their environment. I believe that my active involvement in service provides a continuous opportunity to learn, share knowledge, build networks and relationships and add to my intrinsic job satisfaction. I look forward to continue and develop my effort in service within your institute.