CURRICULUM VITAE

Name: Dr. Shaik Shakeel Ahamad
Mobile: +91-9949235872
E mail:ahamadss786@gmail.com

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 and wireless network technologies

Education

- **Ph.D (Computer Science) full-time** from **University of Hyderabad (UoH) (a Central University), India. Thesis Title: "Design of Protocols for Secure Mobile Payments and their Formal Verification" (Awarded on 3rd Feb 2014)**

- **Master of Computer Applications (MCA)** from during 1996-1999 from Osmania University, Hyderabad, India

- **Bachelor of Science (B.Sc)** with Mathematics, Physics and Electronics during 1992-1995 from Acharya Nagarjuna University, Guntur, India

Employment History

- **October 2013 – Till Date**

  Working as an Associate Professor in Anwarul Uloom College For Computer Science, Hyderabad, AP. (Full Time)

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

- **June 2013- October 2013**

  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)

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

- **August 2007 – May 2013**

  Ph.D (Computer Science) Full Time from University of Hyderabad India. (Full Time)

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

- **Nov 1999 - August 2007**

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

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

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).

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.

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.

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

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

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

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

Research & contribution to the body of knowledge in the area, of Mobile Payments/ Commerce

My proposed mobile payment frameworks are suitable for wireless environments which ensure reliable and end to end communication security (using TCP and TLS) and end to end security at Application layer for financial transactions.

My proposed security frameworks are for two-party and five party mobile payment transactions by employing digital signature algorithms, Signcryption, DSMR (Digital Signature with Message Recovery) mechanisms based on ECC (Elliptic Curve Cryptography) and a Symmetric-key cryptography algorithm (AES).

I have proposed Mobile Traveler’s check (a payment instrument) it has the merits of both e-check and e-cash (i.e. it is as secure as e-check and can be used freely as an e-cash).

I have proposed Mobile payment protocols in MANET environment using Mobile Agents technology and DSMR mechanism by ensuring all the security properties.

I have proposed an enhanced version of SET in mobile environment named EMSET (Enhanced Mobile SET) using Mobile Agents technology and DSMR mechanism overcoming the shortcomings of SET/A, SET/A+ and LITESET/A+ .

I have proposed a Secure Mobile Wallet Framework (SMWF) based on WPKI (Wireless Public Key Infrastructure) and UICC (Universal Integrated Circuit Card) which is a tamper-resistant security-sensitive device, thereby overcoming the demerits of the existing mobile wallet solutions.

I have proposed a Secure and Optimized Proximity Mobile Payment (SOPMP) Framework using NFC by adopting WPKI (Wireless Public Key Infrastructure) and UICC (Universal Integrated Circuit Card) thereby overcoming the demerits of the existing mobile proximity based mobile payment solutions.

The security properties of the proposed protocols in the frameworks are successfully verified using BAN Logic, AVISPA and Scyther Tools.

All the proposed mobile payment protocols are better than the existing protocols in terms of communication cost, computational cost and the number of security properties ensured.

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, UNIX Shell Scripting
- **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), OWASP
- Good Experience in using Fortify Application Security tool.

- Good experience in infrastructure or application-level vulnerability testing and auditing
- Good experience in system, network and/or application security
- Good experience and in-depth technical knowledge of security engineering, system and network security, authentication and security protocols, cryptography, and application security
- Knowledge of network and web related protocols such as TCP/IP, UDP, SSL,TLS, SSH, IPSEC, HTTP, HTTPS, routing protocols
- **Formal Verification Tools:** AVISPA (Automated Validation of Internet Security Protocols and Applications), SPAN v1.6 and Scyther 1.0-rc1

LIST OF PUBLICATIONS

Thesis

Design of Protocols for Secure Mobile Payments and their Formal Verification

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 (2013). A Secure and Optimized Proximity Mobile Payment Framework with Formal Verification. *International Journal of E-Services and Mobile Applications (IJESMA)*, 5(4) (IGI Global Publications) ***((Accepted) (in Press) 2013)*** **(Indexed by DBLP, Scopus)**

6. Shaik Shakeel Ahamad., Sastry, V.N. and Udgata, S.K. (2013). Secure Mobile Payment Framework based on UICC with Formal Verification. *International Journal of Computational Science and Engineering (Special Issue on Future Trends in Security Issues in Internet and Web Applications)* ***(Accepted) (in Press) 2013)*** (Inderscience Publications) http://www.inderscience.com/info/ingeneral/forthcoming.php?jcode=ijcse **(Indexed by ACM Digital Library, DBLP, Scopus)**

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 & Scopus), 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)* (pp.239-246) **NIT Allahabad**. **(Indexed by IEEE Digital Library, ACM Digital Library & Scopus), ISBN:** 978-1-4799-1569-9
4. Shaik Shakeel Ahamad, Siba K. Udgata; Madhusoodhnan Nair (2013). A Secure Lightweight and Scalable Mobile Payment Framework. Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013 Advances in Intelligent Systems and Computing Volume 247, 2014, pp 545-553, (Nov 14th to 16th 2013, Bhuneshwar, India **(Indexed by Springer, DBLP and Scopus)**
5. Shaik Shakeel Ahamad, Sastry, V.N.; Siba K. Udgata; Madhusoodhnan Nair (2013). A Secure and Reliable Mobile Banking Framework. Proceedings of the 48th Annual Convention of Computer Society of India- Vol II, ICT and Critical Infrastructure: Advances in Intelligent Systems and Computing Volume 249, 2014, pp 741-748. Computer Society of India Conference (CSI) in Vizag. **(Indexed by Springer, DBLP and Scopus)**.
6. Shaik Shakeel Ahamad; Madhusoodhnan Nair and Biju Varghese (2013). A Survey on Crypto Currencies. *Proc. Of Fourth Int. Conf. on Advances in Computer Science, AETACS2013 held from* 13th **Dec to 14th Dec 2013 at** NCR. pp 42-48. *DOI: 02.AETACS.2013.4.131*
7. 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
8. 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
9. 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

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.

Awards & Recognition

a) Stood Second in the Ph.D (Computer Science) entrance test and Interview conducted by University of Hyderabad in 2007

b) Talk given on “Network Programming using C and Java” for Scientists of DRDO New Delhi from 15th -17th June 2011

c) 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

d) **Reviewer of** International Journal of Network Security, International Journal of E-Services and Mobile Applications (IJESMA) and Information Security Journal: A Global Perspective Journals and The International Conference of Digital Enterprise and Information Systems (DEIS 2011) conducted by London Metropolitan Business School, United Kingdom.

Personal Information

Date of Birth: 13/07/1975

Father’s Name: John Ahamad

Father’s Occupation: Fitter

Mother’s Name: Khudisiya Begum

Gender: Male

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

Marital Status: Married

Spouse Name: Fatima Masood

Children: Shaik Sheena Ahmed (Daughter)

Residential Address:

Flat No: 302, S.K. Noble Plaza, Beside S.S. Function Hall, Old Mallepally,

Hyderabad-500001, Mob No: +91-9949235872,

Email:ahamadss786@gmail.com

University Address:

Institute for Development & Research in Banking Technology (IDRBT),

Road No 1, Castle Hills, Masab Tank, Hyderabad-500057, India

&

School of Computer and Information Sciences (SCIS),

University Of Hyderabad, Gachibowli, Hyderabad, India

References

- **Prof.V.N.Sastry**

  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**

  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**

  School of Computer and Information Sciences,

  University of Hyderabad, Gachibowli, Hyderabad, India

  Email:crrsm@uohyd.ernet.in

  Phone: +91-040-23010780

Statement on Philosophy of Teaching

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.

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.

Research Statement

Current Research:

My research interests are in the areas of Wireless communications, Application layer security, Data Security, Mobile Commerce and Formal Methods. My research work proposes mobile payment frameworks suitable for wireless environments which ensure reliable and end to end communication security (using TCP and TLS) and end to end security at Application layer for financial transactions. The proposed security frameworks are for two-party and five party mobile payment transactions by employing digital signature algorithms, Signcryption, DSMR (Digital Signature with Message Recovery) mechanisms based on ECC (Elliptic Curve Cryptography) and a Symmetric-key cryptography algorithm (AES). Multifactor Authentication mechanisms (such as NRP & Digital Signatures) are employed for strong authentication. Mobile payment frameworks are proposed in tamper-resistant security-sensitive devices such as SIM and UICC. Mobile payment solutions are proposed in the memory of UICC i.e. client's credentials are stored in the WIM of UICC (with PKI functionality) which is personalized by the client, Mobile Payment Applications are personalized by the banks. Mobile Traveler's check (a payment instrument) is also proposed, traveler's check has the merits of both e-check and e-cash (i.e. it is as secure as e-check and can be used freely as an e-cash). Mobile payment protocols are also proposed in MANET environment using Mobile Agents technology and DSMR mechanism by ensuring all the security properties. My research work proposes an enhanced version of SET in mobile environment named EMSET (Enhanced Mobile SET) using Mobile Agents technology and DSMR mechanism overcoming the shortcomings of SET/A, SET/A+ and LITESET/A+ . This thesis proposes a Secure and Optimized Mobile based Merchant Payment (SOMMP) framework using Signcryption scheme with Forward Secrecy (SFS) based on elliptic curve which consumes less computational and communication cost. SOMMP overcomes the demerits of Tellez et.al protocols. My research proposes a Secure Mobile Wallet Framework (SMWF) based on WPKI (Wireless Public Key Infrastructure) and UICC (Universal Integrated Circuit Card) which is a tamper-resistant security-sensitive device, thereby overcoming the demerits of the existing mobile wallet solutions. My research also proposes a Secure and Optimized Proximity Mobile Payment (SOPMP) Framework using NFC by adopting WPKI (Wireless Public Key Infrastructure) and UICC (Universal Integrated Circuit Card) thereby overcoming the demerits of the existing mobile proximity based mobile payment solutions. Proposed mobile payment frameworks ensures all the security properties (Authentication, Integrity, Confidentiality and Non Repudiation) achieves Identity protection from merchant and Eavesdropper, achieves Transaction privacy from Eavesdropper and Payment Gateway, achieves Payment Secrecy, Order Secrecy, forward secrecy, and prevents Double Spending, Overspending and Money laundering. In addition to these our proposed mobile payment frameworks withstands Replay, Man in the Middle and Impersonation attacks. The security properties of the proposed protocols in the frameworks are successfully verified using BAN Logic, AVISPA and Scyther Tools. All the proposed mobile payment protocols are compared with related works and found to be better than the existing protocols in terms of communication cost, computational cost and the number of security properties ensured.

Future Research Plan:

A) 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 3G 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.

Research Questions to be answered:

Security for MCC should be ensured internally and during the transit of data from client to MCC.
Where should be Mobile Cloud computing implemented in the client side (i.e. in the memory of mobile phone or SIM)?

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.

Internal Security of MCC:

How MCC provider will provide authentication and integrity over user’s data?
How MCC provider will protect stored users data in cloud storage servers form attackers. And how to protect private data from access of hackers whose aim is to hack the servers for access over private data?

During the transit of data from client to MCC:

MCC relies on service concept to deliver computing. In other words when a user requests computing resources he does not need to buy these products but rather can rent a service from a service provider to meet his objectives. Security shows up as a main concern in mobile cloud computing as data should be transferred from the mobile client to the cloud service provider. Since GSM network is the most popular environment for mobile commerce.

How application layer security is ensured in mobile payment and mobile commerce?

Flaws in the design of security protocols:

Secure protocols need to be designed for transferring data between the client and MCC. A protocol is a set of rules that follows the defined conventions to establish semantically correct communications between the participating entities. A security protocol is an ordinary communication protocol in which the message exchanged is often encrypted using the defined cryptographic mechanisms. The network is assumed to be hostile as it contains intruders with the capabilities to encrypt, decrypt, copy, forward, delete, and so forth. Considering an active intruder with such powerful capabilities, it becomes extremely difficult to guarantee proper working of a security protocol. Several examples show how carefully designed protocols were later found out to have security breaches. So how to detect flaws in the protocols

How can we trust that the protocols designed for mobile commerce in MCC are free from flaws?

Privacy/Anonymity: Will mobile cloud computing ensure privacy/anonymity in addition to security?

Cybercrimes in MCC: Several threats may compromise the service or the contract between clients and MCC providers. Despite the use of traditional security defense mechanisms, cybercrimes on MCC infrastructure may always occur. It is therefore crucial to implement forensics techniques to help investigate cybercrime when they do happen.
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?

Autonomic Computing Systems in MCC: Autonomic Computing Systems are systems which are capable of adapting themselves to changes in their working environment in order to maintain required service level agreements, protect the execution of the system from external attacks or prevent and recover from failures. Characteristics of Autonomic computing are self healing, self configuring, self optimization and self protection.
How can MCC be self healable, self configurable, self optimized and self protectable?

Technical approach of how and what R&D in MCC work will be carried out: My approach is to design secure mobile commerce protocols based on MCC by adopting Wireless Public Key Infrastructure (WPKI) using UICC as a secure element from client’s side. Designed mobile commerce protocols must ensure end-to-end security i.e. from the mobile client’s device to the MCC. MCC based payment solutions will assist in securing merchants and developers of applications requiring payments from the risk of data breach, Expertise in data security, particularly Payment Card Industry (PCI), Platforms that give speed to market and access to all and Reduce merchants PCI (Payment Card Industry) scope by never seeing or storing payment card data in the clear. Merely using cryptographic mechanisms, does not guarantee security-wise semantically secure operation of the protocol, even if it is correct. There indeed have been reported breaches in the security protocols, after being published and accepted as a safe protocol. Therefore the design of security protocol is an intuitive process which is severely error-prone so a more rigid framework is required within which we can safely design secure protocols. In order to gain confidence in the cryptographic protocol employed, it is desirable that the protocol be subjected to an exhaustive analysis that verifies its security properties. Some of the tools developed for the purpose are Scyther [17] and AVISPA [18]. So we have verify our proposed mobile commerce protocols based on MCC using Scyther [17] and AVISPA [18] tools. Our proposed mobile commerce protocols based on MCC ensures Authentication, Integrity, Confidentiality and Non Repudiation, achieves Identity protection from merchant and Eavesdropper, achieves Transaction privacy from Eavesdropper and Payment Gateway, achieves Payment Secrecy, Order Secrecy, forward secrecy, and prevents Double Spending, Overspending and Money laundering. In addition to these our proposed protocol withstands Replay, Man in the Middle and Impersonation attacks. Our proposed framework will overcome Identify security threats and cybercrime in MCC environment. MCC in our proposed framework will be self healable, self configurable, self optimized and self protectable. In addition to these virtual servers of Sun Enterprise T5240 based on Apache Hadoop and Google AppEngine in order to provide services for the consumption on various mobile clients including the Android devices such as Motorola Droid/Milestone and HTC Hero or the Apple iPhone. Technologies used are Android SDK, GAE SDK, JavaScript, HTML, virtualization technologies, Amazon Web Services.

B) MOBILE HEALTH CARE

To propose and verify secure protocols in the realm of Mobile Health Care using Formal Verification Tools.

Real Time Projects Implemented:

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

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

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)

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)

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)

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)