Project List

1. **Project Name: Efficient Anonymous Private Authentication Protocol for RFID Systems**

Project Summary: Privacy protection is a very important issue during authentications in RFID systems. One limitation of existing technique is that the level of privacy provided by the scheme decreases as more and more tags are compromised. Therefore, in this paper, we propose a group based anonymous private authentication protocol (AnonPri) that provides higher level of privacy than the above mention group based scheme and achieves better efficiency than the approaches that prompt the reader to perform an exhaustive search. Our protocol provides unlinkability and thereby preserves privacy. The adversary cannot link the responses with the tags, even if she can learn the identifier that the tags are using to produce the response. To evaluate AnonPri, we have compared both the protocols, AnonPri and the group based authentication. The experiment results establish that the level of privacy provided by AnonPri is higher than that of the group based authentication.

Publication:

- Md. Endadul Hoque, **Farzana Rahman**, and Sheikh I. Ahamed, "**AnonPri: An Efficient Anonymous Private Authentication Protocol**", *in Proc. of the IEEE International Conference on Pervasive Computing and Communications (PerCom 2011),* WA, USA, March 2011. pp.102-110. *[Acceptance rate: 11%].*

2. **Project Name:** ***EcoDrive: Development of a Mobile Tool to Reduce Carbon Footprint and Promote Green Transport***

Project Summary: In this project, we developed a mobile GPS application, EcoDrive, for iPhone that suggests the fuel efficient route to the user. The EcoDrive application runs on Apple iPhone running the iOS operating system and is programmed in Objective C. The data stored on the application side uses Apple's Core Data framework. The application references Google's mapping API to display the map and resolve location using the built in geocoding. Our server side runs a LAMP (Linux Apache MySQL PHP) stack and is programmed in PHP. We have also developed web services as part of OCFF framework. The framework's API processes requests based on the REStful web services protocol. The framework uses eferences Google's geocoding and mapping API.

Publication:

- **Farzana Rahman**, Casey O'Brien, Sheikh I. Ahamed, He Zhang and Lin Liu, "**Design and implementation of an open framework for ubiquitous carbon footprint calculator applications**", *Elsevier Journal of Sustainable Computing: Informatics and Systems, Volume 1, Issue 4,* December 2011. pp. 2210-5379. http://dx.doi.org/10.1016/j.suscom.2011.06.001
- **Farzana Rahman**, Casey O'Brien, Kristine Manning, Jason Cowdy, Sheikh Iqbal Ahamed, "**Let EcoDrive be Your Guide: Development of a Mobile Tool to Reduce Carbon Footprint and Promote Green Transport**", to appear in *Proc. of ACM Symposium on Applied Computing (SAC 2012)*. Italy, 2012.

3. **Project Name:** ***PCO: A Privacy Sensitive Architecture for Context Obfuscation***

Project Summary: Privacy in a pervasive online community depends on the level of granularity of the provided information, the number of and the user's relation to possible recipients, and the possible usage of the user's data, Conventional privacy preservation techniques are not suitable for these pervasive applications. We proposed a novel Privacy-sensitive architecture for Context Obfuscation (PCO) for privacy preservation in pervasive online community based applications. More specifically, PCO safeguards a user's privacy by generalizing the contextual data (e.g. the user's current activity) provided to the applications and distributed to the user's peers. To support multiple levels of granularity for the released contextual data, the obfuscation procedure uses an ontological description that states the granularity of object type instances. We have developed and evaluated a contextual instant messaging application that incorporates level-based privacy of the user's contextual information.

Publication:

- **Farzana Rahman**, Md. Endadul Hoque, Ferdous Kawser, and Sheikh Iqbal Ahamed, "**Preserve Your Privacy with PCO: A Privacy Sensitive Architecture for Context Obfuscation for Pervasive E-**

Community based applications", in *Proc. of the International Conference on Social Computing (SocialCom10)*, MN, USA, 2010. pp.41-48. *[Acceptance rate: 13%].*

4. **Project Name:** ***Towards Anonymity Protection with Privacy Quantification for Context-aware Applications***

Project Summary: Context-based pervasive applications have the vulnerabilities of tracking and capturing extensive portions of users' activities. So, users certainly desire to be notified of potential data capture. Whether such data capture is an actual threat or not, users' perceptions of such possibilities may discourage them from using and adopting pervasive applications. So far in context-based pervasive applications, location data has been the main focus to make users anonymous. However in reality, anonymity depends on all the privacy sensitive data collected by the applications. Protecting anonymity with the help of an anonymizer has the susceptibility of a single point of failure. We propose a formal model that preserves users' anonymity without anonymizer while quantifying the amount of privacy at the time of asking for services from untrustworthy service providers. Before placing a request, each user can protect his own anonymity by collaborating with his peers. In addition, we introduce a novel approach to quantify the requester's achieved privacy by the request to be placed. Finally we present an experimental evaluation of our proposed model.

Publication:

- **Farzana Rahman**, Md. Endadul Hoque, and Sheikh I. Ahamed, "**ProQuPri: Towards Anonymity Protection with Privacy Quantification for Context-aware Applications**", in *Proc. of the ACM Symposium on Applied Computing (ACM SAC 2011)*, Taiwan, March 2011.

5. **Project Name:** ***REBIVE: A Reliable Private Data Aggregation technique for Wireless Sensor Networks***

Project Summary: In WSNs, achieving ideal data accuracy is complicated due to collision, heavy network traffic, processing delays and/or several attacks. The problem of gathering accurate integrated data will be further intensified if the environment is adverse. Hence how to attain data privacy and perfect data accuracy are two major challenges for data aggregation in wireless sensor networks. To address this problem, we designed a new privacy preserving data aggregation scheme, REBIVE (REliaBle prIVate data aggrEgation scheme). In REBIVE data accuracy maintenance and data privacy protection mechanisms work cooperatively. Different from past research, our proposal have the following features: providing privacy preservation technique for individual sensor data and aggregated sensor data; maintaining perfect data accuracy for realistic environments; being highly efficient; and being robust to popular attacks launched in WSNs.

Publication:

- **Farzana Rahman**, Md. Endadul Hoque, and Sheikh I. Ahamed, "**REBIVE: A Reliable Private Data Aggregation Scheme for Wireless Sensor Networks**", *in Proc. of the ACM Symposium on Applied Computing (ACM SAC 2011)*, Taiwan, March 2011. pp. 439-444.

6. **Project Name:** ***Priloc: Automated transportation system using location based services***

Project Summary: Location Based Services (LBSs) are information services accessible with mobile devices through the mobile network and utilizing the ability to make use of the location of the mobile device. The LIMO service is a heavily used and vital service providing safety and convenience to the Marquette community. In this project, some important improvements of traditional transportation system were identified by observing the LIMO service of Marquette University. Also a research survey was conducted on existing LBSs' to find out research issues. For the design of a complete automated transportation system, a unique set of web services have been identified. A preliminary prototype of PriLoc is developed and applied to improve traditional transportation system. Finally user evaluation is collected in response to the algorithms we have developed.

7. **Project Name:** ***CFC: Being green with real time Carbon Footprint Calculator***

Project Summary: Low carbon emission and environment friendliness is one of the most commonly mentioned non-functional requirements for building IT systems. From a software engineer's point of view, there is a main issue in which we can contribute to. We name it a Green Software Infrastructure. As a first step towards green software infrastructure, we developed an individual carbon footprint calculator application. Conducted an extensive research survey to find out the important parameters of carbon emission from users' perspective. Identified different parameters which can contribute to the carbon footprint of an individual person. Used low cost and reusable sensors to collect the parameter values from the environment and finally used a mathematical model to determine the real-time carbon footprint of a person.

Publication:

- **Farzana Rahman**, Sheikh Iqbal Ahamed, Md. Endadul Hoque, Casey O Brian, Lin Liu, He Zhang, "**UCFC Ubiquitous Personal Carbon Footprint Calculation Platform**", *in Proc. of the Workshop for The Work in Progress in Green Computing:(WIPGC 2010)*, Chicago, IL, USA, 2010.
- He Zhang, Lin Liu, Sheikh Iqbal Ahamed, and **Farzana Rahman**, "**Open Carbon Footprint Calculation Platform for Personal Users**", *in Proc. of the Second International Workshop on Software Research and Climate Change (ICSE 2010)*, South Africa, 2010.

8. Project Name: *Ensuring security, privacy and robustness of RFID Authentication*

Project Summary: Ensuring strong privacy and security has been an enormous challenge due to extremely inadequate computational storage of typical RFID tags. So usually in order to relieve tags from responsibility, privacy protection and security assurance was guaranteed by central server. We suggested serverless, forward secure, anonymous and untraceable authentication protocol for RFID tags. This authentication protocol safeguards both tag and reader against almost all major attacks (such as: Privacy protection, Eavesdropping, Tracking, Cloning, Physical attacks, Se-synchronization and Denial of Service) without the intervention of server. It is also critical to guarantee untraceability and scalability simultaneously. We proposed a scheme to make our protocol more scalable by using the concept of ownership transfer.

Besides thwarting some major attacks, RFID systems need to be able to recover from unexpected conditions during operation. In an advanced work of this project, we proposed a Robust Authentication Protocol (RoAP) that supports not only security and privacy, but also recovery in RFID systems. The protocol can get back the desynchronized tags and readers to their normal state, and thus provides robustness. Identified a "safety ring" which consists of six major goals that have to ensure by each RFID system to be secured. Performed an enhanced security and robustness analysis of the protocol.

Performed further investigation for designing a hexagonal cell based distributed architecture which ensures improved scalability while maintaining privacy. The hexagonal architecture allows readers to co-operate with one another to identify tags without compromising scalability. Furthermore, this architecture uses serverless protocols for security assurance, cutting down set up and maintenance cost as well as traffic to server.

Publication:

- **Md. Endadul Hoque**, Farzana Rahman, Sheikh I. Ahamed, and Jong Hyuk Park, "**Enhancing Privacy and Security of RFID System with Serverless Authentication and Search Protocols in Pervasive Environments**", *Springer Wireless Personal Communication*, 2009, http://dx.doi.org/10.1007/s11277-009-9786-0.
- **Md. Endadul Hoque**, Farzana Rahman, and Sheikh Ahamed, "**Supporting Recovery, Privacy and Security in RFID Systems Using a Robust Authentication Protocol**", in Proceedings of the 24th ACM Symposium on Applied Computing (ACM SAC 2009) , Hawaii, USA, March 2009, pp. 1062-1066.
- Sheikh I. Ahamed, Farzana Rahman, **Endadul Hoque**, Fahim Kawsar, Tatsuo Nakajima, "**YA-SRAP: Yet Another Serverless RFID Authentication Protocol**", in *Proceedings of the 4th IET International Conference on Intelligent Environment (IE08)*, Seattle, USA, July 2008, pp. 1-8.
- Sheikh Iqbal Ahamed, Farzana Rahman, and **Md. Endadul Hoque**, "**Secured Tag Identification Using EDSA (Enhanced Distributed Scalable Architecture)**", in *Proceedings of the 23rd Annual ACM Symposium on Applied Computing (ACM SAC 2008)*, Ceará, Brazil, March 2008, pp. 1902-1907.

9. Project Name: *Ensuring security, privacy and scalability of RFID tag Searching*

Project Summary: Since RFID tags are extremely constrained in time and space, enforcing high level of security with excessive cryptographic computation is not possible. One extension of RFID authentication is RFID tag searching. But we firmly believe that in near future tag searching will be a significant issue. And tag searching need to be scalable as RFID tags are deployed comprehensively within a system. Under this project, we proposed a lightweight RFID tag searching protocol. The protocol can search a particular tag efficiently as the approach is not based on exhaustive search and it does not employ extreme cryptographic functions.

As a further extension of this project we investigated the scalability issue of RFID systems. Tag searching need to be scalable as RFID tags are deployed comprehensively within a system. We proposed scalable, forward secure, anonymous, and secure search (*S-Search*) protocol for searching RFID tag. The *S-Search* protocol does not require the reader to collect IDs from each RFID tag, but is still able to accurately find out a specific RFID tag. The search protocol uses slotted ALOHA technique for reply transmission.

Publication:

- Sheikh I. Ahamed, Farzana Rahman, **Endadul Hoque**, Fahim Kawsar, and Tatsuo Nakajima, "**Secure and Efficient Tag Searching in RFID Systems using Serverless Search Protocol**", *International Journal of Security and Its Applications (IJSIA)*, Vol.2, No.4, October 2008.
- **Md. Endadul Hoque**, Farzana Rahman, and Sheikh I. Ahamed, "**S-Search: Finding RFID Tags Using Scalable and Secure Search Protocol**", to appear in *Proceedings of the 25th ACM Symposium on Applied Computing (ACM SAC 2010)*, Switzerland, March 2010.
- Sheikh I. Ahamed, Farzana Rahman, **Endadul Hoque**, Fahim Kawsar, and Tatsuo Nakajima, "**S^{3}PR: Secure Serverless Search Protocols for RFID**", to appear in *Proceedings of the Second IEEE International Conference on Information Security and Assurance (ISA 2008)*, Busan, Korea, April 2008, pp. 187-192.

10. Project Name: *ERAP: Secure RFID authentication protocol based on Elliptic Curve Cryptography (ECC)*

Project Summary: RFID has gained appreciation as an emerging technology to thwart counterfeiting problem. And public key cryptography (PKC) provides impeccable solution to the counterfeiting problem. One recent family of public key cryptosystem is Elliptic curve cryptography (ECC) which is a better choice than RSA cryptographic system because of its shorter key length. Moreover depending upon the environment and application in which it is used, improved performance can be achieved. We adopt the belief that ECC based public key algorithms are feasible for RFID identification or authentication. We proposed ECC based RFID authentication protocol (ERAP) which is secure against some major passive and active attacks. This is a mutual offline authentication protocol which ensures that the tag and the reader authenticate each other prior to any data exchange.

Publication:

- Sheikh Iqbal Ahamed, Farzana Rahman, and **Md. Endadul Hoque**, "**ERAP: ECC based RFID Authentication Protocol**", in *Proceedings of the 12th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS 2008)*, Kunming, China, October 2008, pp. 219-225.

11. Project Name: *Secured initial trust in pervasive environments*

Project Summary: Trust models play a major role in guarding against privacy violations and security breaches. Though assignment of initial trust is an important issue, little work has been done in this area. Most of the prior researches on trust models assume a constant level of the initial trust value. However, in a pervasive smart space, trust is context dependent. The need for security varies from context to context. In addition, some services, being shared in this environment, require high security while sharing. To ensure this, security levels should be incorporated in the initial trust calculation. We propose a new initial trust model called ICSTB (Integration of Context Security in Trust Bootstrapping). The model categorizes services or contexts in different security levels based on their security needs, and these security needs are considered in trust bootstrapping.

As an extension of this project we also developed Adaptive Initial trust and Demand aware Secure Resource Discovery (AID-SRD) model for pervasive environment. Traditional computer systems and small distributed networks rely on users' authentication to provide security. However, this strategy is extremely inadequate for the increased flexibility of pervasive environments, where users join and leave frequently. We proposed a solution to this using a secure resource discovery model AID-SRD. Incorporated a Demand Unit in AID-SRD which enables efficient resource sharing with unknown devices. AID-SRD also assigns initial trust considering the variable security need of different services.

Another extension of this project is the presentation of a context specific and reputation based trust model along with a brief survey of trust models suitable for peer-to-peer and ad-hoc environment. We have devised a multi-hop recommendation protocol and a flexible behavioral model to handle interactions. One other major contribution of this project is a simple method of handling malicious recommendations. Illustrated the implementation and evaluation of our proposed formal trust model.

Publication:

- Sheikh I. Ahamed, **Endadul Hoque**, Farzana Rahman, and Mohammad Zulkernine, "**Towards Secured Trust Bootstrapping in Pervasive Computing Environment**", in *Proceedings of the 11th IEEE High Assurance Systems Engineering Symposium (HASE 2008)*, Nanjing, China, December 2008, pp. 89-96.
- **Md. Endadul Hoque**, Farzana Rahman, and Sheikh Iqbal Ahamed, "**An Adaptive Initial Trust and Demand Aware Secure Resource Discovery (AID-SRD) Model for Pervasive Environments**", in *Proceedings of the 3rd IEEE International Workshop on Web and Pervasive Security (WPS 2009)* held in conjunction with *PerCom 2009*, Texas, USA, March 2009, pp. 1-6.
- Sheikh I. Ahamed, Munirul M. Haque, **Md. Endadul Hoque**, Farzana Rahman, and Nilothpal Talukder, "**Design, Analysis, and Deployment of Omnipresent Formal Trust Model (FTM) with Trust Bootstrapping for Pervasive Environments**", *Journal of Systems and Software (JSS)*, Elsevier, to appear 2009, http://dx.doi.org/10.1016/j.jss.2009.09.040.

12. Project Name: *Using trust for security auto-configuration in assisted living environments*

Project Summary: For elderly people, conceiving technologies for increasing their autonomy, so as to enable them to self-manage their life is of utmost importance. However, when it comes to smart home, once all appliances in a home are automated and connected through internet, it becomes essential to consider issues of security, especially security configuration. In the smart home, security has to be configured and managed by technology-unaware elderly people. One mechanism of auto security configuration in such environment can be achieved by observing the trustworthiness of smart devices. Trust-based security mechanisms allow access rights to evolve among previously unknown devices, thus minimizing security configuration. We presented a security configuration model which takes critical security decisions by determining the trustworthiness of an entity based on the sources of trust: Direct interaction and Recommendation trust.

Publication:

- **Md. Endadul Hoque**, Farzana Rahman, Sheikh I. Ahamed, and Lin Liu, "**Trust Based Security Auto-Configuration for Smart Assisted Living Environments**", to appear in *Proceedings of the ACM Workshop on Assurable & Usable Security Configuration (SafeConfig 2009)* collocated with *ACM CCS 2009*, Chicago, USA, November 2009.

13. *Project Name: A simulator for predicting ecological transition of lakes*

Project Summary: Eutrophication is an increase in the concentration of chemical nutrients in an ecosystem to an extent that increases the primary productivity of the ecosystem. Though any exact model of eutrophication is unknown, increased variance of water phosphorus level is an important clue of regime shift (an state when lake approaches a transition from oligotrophic to eutrophic). In this project, we developed a software or simulator to predict the timing and progression of Lake Eutrophication using a simulated model. Using Gaussian distribution as initial soil phosphorus level, this simulator can predict the timing in years for a lake to turn from oligotrophic to eutrophic state.