## ICT Project BS Students Positions (for FYP):

### 1. Context Aware Access Control using Extensible Access Control Framework

KTH-Applied Information Security lab is looking for enthusiastic final year students interested in doing final year project as part of ICT R&D funded project titled “Extensible Access Control Framework for Cloud based Applications” which focuses on design and development of an extensible access control framework for applications hosted on Software-as-a-Service (SaaS) layer of Cloud. The main goal of this funded project is to provide Access Control-as-a-Service (ACaaS) that can manage complex access control policies and incorporates multiple access control models in a flexible manner, according to the security needs of Cloud consumers. Therefore, this final year project aims towards the design and implementation of one of the emerging and dynamic authorization model i.e. Context-Aware Access Control model (CAACM) to verify the extensibility of framework. A context is referred to as any information that could be related to a user (e.g. user’s access location) or a system (e.g. network type) and could be static or dynamic. Cloud based applications takes into account the dynamic and static contextual attributes and promptly react to the value changes of the contextual attributes therefore, authorization in Cloud must also be context-aware.

In this regard, Context-Aware Access Control model (CAACM) must be used that takes contextual information into account to reflect the dynamic environment of Cloud. Existing context-aware access control models focus on location and temporal contextual information to constraint access control. However, a holistic context–aware access control model, comprising all the features, is still needed for Cloud specific security requirements. Moreover, CAACM will be implemented using an industry standard for policy specification i.e. Extensible Access Control Markup Language (XACML), which itself is a challenging task, since XACML does not support most of the features of CAACM, Policies will be created and evaluated according to the characteristics of CAACM, using already existing XACML elements. Thus, this FYP will cater the above mentioned problems by specifying and evaluating CAACM policies in XACML 2.0.

**Related Tools & Technologies:** In this FYP, students will use and learn technologies such as Java (Eclipse/Netbeans), MySQL, XACML, Web Services, Tomcat and OpenStack, Amazon EC2.

### 2. Enhanced Usage based Access Control for Cloud based Applications

KTH-Applied Information Security (AIS) lab is seeking FYP interns for the development of extended Usage based Access Control (UCON) model for Cloud based applications. The project aims to provide advance features in UCON model other than the basic features which include design and development of Application independent Context Handler and Usage Monitor and Policy Information Point (PIP). Moreover, UCON updates can be exploited by providing one-time metadata exchange using SAML between the Access Control Provider and Applications so that updates can be application-dependent. The implemented UCON model will be tested on Moodle application, is an open source project for learning management systems that is used by various institutions, including NUST. This FYP is a part of ICT R&D funded project entitled, "Extensible Access Control Framework for Cloud-based Applications," and the chosen candidates will be given remunerations of Rs. 3500/- each.

**Requirements:** The candidates must have general knowledge of Java, MySQL, PHP, XACML, Web Services, Tomcat and WampServer.

## 3. Enhanced Fine Grained Access Control for Cloud based extensible Applications

KTH-Applied Information Security (AIS) lab is seeking FYP interns for the development of extended Fine Grained Access Control (FGAC) model for Cloud based applications. This FYP is a part of ICT R&D funded project entitled, "Extensible Access Control Framework for Cloud-based Applications," and the chosen candidates will be given remunerations of Rs. 3500/- each. The major objective of the project is to offer enhanced functionality of FGAC model so that it can be deployed independently of the underlying Cloud applications using it. For that purpose, independent Context Handler and Policy Information point (PIP) is to be implemented in order to completely dispatch default authorization module of Cloud based applications. One-time FGAC metadata exchange using SAML between the Access Control Provider and Applications is also the intended functionality. The implemented FGAC model will be tested on DSpace which is an open source repository software package. It is typically used for creating open access repositories for scholarly or published digital content.

**Requirements**: Students with interest in Java programming should apply. The development platform will be eclipse/netbeans and the candidates must have general knowledge of Web Services and Tomcat.

## 4. Dynamic Resource Management in g-SIS Environment using GSAKMP

Group Secure Information Sharing environment is well-known for shared use of resources within large, dynamic, multi-institutional communities. This sharing is not limited to file exchange only but includes direct access to computers, software, data, and other resources to perform both individual and collaborative tasks. Different organizations comprise of a complex structure in which groups are created and destructed dynamically based on events or tasks required. For instance in an educational institution, a group is formulated to host a conference/workshop. The existing solutions lack support for centralized requirement based resource sharing and management. In this internship we aim to design & implement a comprehensive and easy to use secure resource management system for Group-Secure Information Sharing (g-SIS) systems. In addition, this internship intends to explore the prospects of using Public-key Infrastructure (PKI) and Group Secure Association Key Management Protocol (GSAKMP) in detail.

## 5. Collaborative framework for group sharing

In a group centric environment, members of a group contribute valuable information or resources with each other for a specific rationale. Sharing of sensitive information/resources among various group members poses the concerns of its security and effective management. Having said that, even if the secure groups have been formed and access to legitimate users has been granted, the provision of dynamic delegation to other users in g-SIS environment still stands as a daunting challenge. Dynamic delegation permits some users to create policies of limited duration to delegate certain capabilities to others. XACML 2.0 allows policies that say, *"Mary can do something on behalf of Jack"* by means of different subjects. But, it would be more useful to allow people to generate policies on the fly that say such things as *"while I am on vacation, Mary can approve requests."* This internship intends to design & implement dynamic delegation framework for g-SIS.

### 6. Cloud based access control decision profile

The policy evaluation performed by an XACML Policy Decision Point (PDP), is generally defined in terms of a single decision request in the XACML Specification, with the authorization decision contained in a single *<Result>* element of the response. A Policy Enforcement Point (PEP), however, may wish to submit a single request context for multiple access control decisions, and may wish to obtain a single response context that contains a separate authorization decision *(<Result>)* for each requested decision. Such a request context might be used to avoid sending multiple decision request messages between a PEP and PDP. In addition, PEP may wish to submit a single request context for multiple decisions, and may wish to obtain a single authorization decision *(<Result>)* that indicates whether access is permitted to all of the requested decisions. Considering the performance and efficiency requirements, there is a need to design and implement a multiple decision framework and for that we need to explore several ways in which a PEP can request multiple authorization decisions in a single request context, and how the result of each such authorization decision is represented in the single response context that is returned to the PEP. In this internship, we aim to design and implement an XACML 3.0 based multiple decision framework.

## Internship Positions:

### 1. Security-as-a Service for Column Oriented NoSQL Databases in Cloud

KTH-Applied Information Security (AIS) lab is seeking an intern for a project entitled "Security-as-a-service for Column Oriented NoSQL databases in Cloud". Column oriented NoSQL databases are one of the increasingly popular databases in Cloud since they provide flexibility, scalability, and performance as required by most of the next generation applications. Sharing of sensitive data among such Clouds databases poses the concerns of its security, privacy and access control. Hence, our objective for this project is to address such issues by ensuring security features particularly for Column based NoSQL databases. These features will be deployed as a service in a Cloud environment.

This internship offered by the AIS lab will serve as a practical introduction to the security issues of column oriented NoSQL databases. The internee would need to implement and deploy a complete system using the Fine Grained Access Control model for providing column level authorization. Furthermore, strong authentication mechanisms, data at rest encryption as well as secure key management are other sub modules of this project. Cassandra database will serve as a test bed for this project.

**Requirements**: Students with interest in Java programming should apply. The development platform will be eclipse and the candidate must have general knowledge of databases.

### 2. Enhancing Trust in Cloud Federation by Using the Risk Based Access Control

KTH-Applied Information Security (AIS) lab is seeking an intern for the project titled *Enhancing Trust in Cloud Federation*. Cloud computing has revolutionized the computing paradigm but still there a number of security issues that need to be addressed. When it comes to cloud federation, trust is considered to be a salient parameter; trusting a cloud service provider whether it is providing the services that are desired is a big question. In this regard, we have proposed a trust evaluation framework; our proposed framework uses risk based access control to access or deny the request of a subject to the resource. The internship will require the implementation of risk based access control using the *eXtensible access control markup language* (XACML) and its deployment in a cloud environment. This project will serve as introduction to cloud domain and will give hands on experience to the eXtensible access control markup language. The summer internship may lead to FYP based on performance.

**Requirements:** Students with interest in Java programming should apply. Eclipse/Netbeans will be used as the development platform.

## 3. Secure Sharding in Cloud Federation

KTH-Applied Information Security (AIS) lab is seeking an intern for the "Secure Sharding in Cloud Federation" project. In Cloud DBaaS model, client's sensitive data has to reside on cloud provider's domain. This needs for extra security measures on provider's side to guard client's data privacy as most big clients (corporations, enterprises etc) view their data as a valuable asset. This project aims to provide effective access control and data encryption in MongoDB to ensure the security of unstructured data residing on domains of multiple cloud providers. The proposed solution will offer user authorization, data security, encryption key security and load balancing by using MongoDB's existing sharding architecture.

This summer internship will require embedding of collection level fine grained access control (using XACML) for user authorization, field level encryption (using Cryptopp library) and storage of user data across cloud federation along with the management of cryptographic keys in the C++ based open source implementation of NoSQL database MongoDB. The solution will not only provide security of data-at-rest but also data transmission security across MongoDB sharded data stores. The summer internship may lead to FYP based on performance.

**Requirements:** Students with interest in C++ programming should apply. The development platform will be Microsoft Visual Studio 2010.

## 4. Distributed Intrusion Detection System using Mobile Agents in Cloud Computing Environment (DIDMACC)

Cloud Computing is an emerging technology of today that is rapidly being adopted by many IT organizations due to its open and distributed architecture. The main features of cloud computing are cost effectiveness, scalability, and ubiquity. However, security is a major concern that makes people uncertain about whether or not to use cloud services. Particularly, intruders can break into a cloud based network and violate the confidentiality, integrity and availability of cloud users and services. This urges the need of Intrusion Detection System (IDS) that is an effective security mechanism, setup in cloud to successfully detect intrusions. IDS may be deployed at Infrastructure as a Service

(IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) layers of cloud. However, IDS setup at IaaS layer of cloud is the most flexible solution since IaaS provides you more options as a consumer.

This internship leading to final year project focuses on use of various open source tools to detect distributed intrusions in cloud based network. We will use ***suricata (an open source Network based IDS)*** to monitor the network packets coming in/ going out of a VM's network interface and analyze them to detect intrusions. We have used ***Java Agent DEvelopment Framework (JADE)*** for development of mobile agents. The Java based mobile agents carry intrusion alerts from VMs to Management Station (MS) for correlation of intrusion alerts. Correlation is accomplished using ***OSSIM (Open Source Security Information Management)*** correlation module. After correlation and successful detection of a distributed intrusion, MS generates an alert to system admin who takes appropriate action. It also sends the signature of newly detected distributed intrusion to other VMs so that they can update their local database and can avoid such intrusions in future.

**Related Tools & Technologies:** Apache CloudStack, Suricata, MySQL Database, Java
(Eclipse/Netbeans), OSSIM