CST4125: Blockchain Development
Week: 3
Title: Access Control

Dr Ian Mitchell

smerf.net
Bedfordshire,
UK

2023

Contact and Office Hours

Contact Details

- Name: Dr Ian Mitchell
- Room: TG10
- Address: Middlesex University, Computer Science, London, NW4 4BT
- email: `smerf.net`

Contact and Office Hours

Contact Details

- Name: Dr Ian Mitchell
- Room: TG10
- Address: Middlesex University, Computer Science, London, NW4 4BT
- email: `smerf.net`

Office Hours

- During term time only
- When: Winter Term: Mondays 1100-1300hrs
- Please read notifications or emails
- There are occassions that these could be arranged online, e.g., due to industrial action or inclement weather

Deadlines

				Feedback	
Description	Submission	Weight	Deadline	Formative	Summative
1. Hyperledger	MyLearning	50%	14th April 2023	LW11-12	10/05/2023
2. Ethereum	MyLearning	50%	8th July 2023	LW23-24	28/07/2023
Resits	MyLearning	50-100%	14th August 2023	None	None
Deferals	MyLearning	50-100%	14th August 2023	None	None

Coursework 1

- Problem Definition: 14%
- Data Modelling: 18%
- Access Control Language: 16%
- Business Logic: 26%
- Documentation: 4%
- Presentation: 20%
- Business Network Archive: 2%
- **Deadline: 14th April 2023**

Problem Definition: 14%

Criteria	Sub-criteria	0	1	2	3	4	W	Σ
Problem Definition, PD (14%)	Specification	No Spec.	Spec., present	Spec. is not conducive to BC	Unrelated or missing spec. components	Spec. conducive to BC, all components explained and coherent	1	/4
	Flowchart, FC	No use of FC in **[yaga2018blockchain]**	FC applied, no explanation.	All components of FC applied, some explanation.	All components of FC applied correctly but does not match spec/UCD.	All components of FC applied correctly and matches spec/UCD	1	/4
	Use Case Diagram, UCD.	No UCD	Incoherent UCD	Misaligned UCD and PD. Assumptions left uncommented	No include or extend relationships. Assumptions commented	Aligned and complete UCD with comments and assumptions	1	/4

Data Modelling: 18%

Criteria	Sub-criteria	0	1	2	3	4	W	Σ
Data Model (18%)	Participants	No participants	Lacking and/or incorrect participants. Incorrect data types used. Unidentified.	Irrelevant participants. Correct identification. Lacking any assumptions. Opportunities to use more appropriate data types missed.	Participants lacking UCs and incomplete assumptions. Structurally sound.	Correct participants, data structures, assumptions and matching UCs	1	/4
	Assets	No assets	Lacking and/or incorrect assets	Irrelevant assets. No enum or concepts.	Assets unrelated to participants or no assets with the capability of state change	Some of the assets must at least be 3 of the following: have a state capable of change, relevant, complete and related to participants	1	/4
	Transactions, TX	No TX	Vague TX	TX not updating state	TX without ownership	participant specific TX	1	/4
	Comments	No comments	Auto-generated comments only (headers only), no clarifying comments	Vague, incorrectly placed and/or unexplanatory comments	Explanatory and identifiable comments, but incomplete. Too verbose and high comment to code ratio	Complete, concise and succinct comments	1	/4

Access Control Language: 16%

Criteria	Sub-criteria	0	1	2	3	4	W	Σ
Access Control Language, ACL, (16%)	Participants	No ACL. Basic ACL, admin access only & automatically generated code	ACL has too few rules	ACL has contradictions or allows unauthorised access to transactions or assets. There is no difference between participant access	ACL order is incorrect	ACL is implemented correctly	1	/4
	Ordering, Comments and listing	No listing or basic ACL, admin access only & automatically generated code	Syntax errors for ACL.	Rules are disorganised and need re-ordering. Inclusion of commented out rules	Rules are in correct order, but lack ideal names, descriptor values and comments. No line numbers.	Correct order and appropriate names, descriptors values and comments	1	/4
	Conditions	Auto-generated rules only. Admin access to all.	No conditions and simple rules only	Conditions applied incorrectly.	Identifier conditions applied correctly	Conditions to check status or lists and of a higher order of difficulty	1	/4

Business Logic: 26%

Criteria	Sub-criteria	0	1	2	3	4	W	Σ
Business Logic (26%)	Queries	No Queries	Queries but don't execute	Irrelevant Queries	Relevant Queries without relationships	Relevant Queries with relationships	1	/4
	Transactions	No Transactions	BL - run time execution	BL code accessing assets and participants, with no restriction, or comments directing to ACL	BL code accessing TX with restrictions, but not acknowledged	Acknowledged rules and restrictions and code accessing both assets and participants correctly	2	/8
	API	No use of promises	BL code not executing	BL code duplicating ACL	No extensive use of API and promises	Extensive use of API and Promises and complexity used to aid the update of state correctly	3	/12
	Initialise	No initialisation or automatic population of values in registry	Initialisation present but not working	Initialisation only partial, e.g., only completes assets and not participants	All assets and participants populated but incorrectly, e.g., data is misaligned	All assets and participants populated correctly	1	/4
	Comments	No comments	Non-explanatory comments	Partial explanatory comments	Overly commented	Fully explanatory comments	1	/4

Presentation: 20%

Criteria	Sub-criteria	0	1	2	3	4	W	Σ
Presentation (20%)	Slide Content	No slides	Incoherent presentation and not demonstrating the understanding of the coursework. Cluttered and/or illegible slide content	Coherent but poor content coverage. Less than 5 mins in length. Uncluttered. Some Illegible slide content, especially screenshots	Less than 9 mins or greater than 10 mins. Clear figures and screenshots. Coherent but not explaining all points required	Between 9-10 mins in length, clear and readable slides and addresses all items	1	/4
	Transaction, TX	No Demonstration	Demonstration of successful TX	Demonstration of unsuccessful TX due to ACL	Demonstration of unsuccessful Demonstration due to BL	All demonstrations completed	1	/4
	Structure	No structure	No headers *and* footers, slide numbers	No headers *or* footers, slide numbers	Headers, Footers and numbers but incorrect	All slides consistent with correct information in headers and footers.	1	/4

Documentation: 4%

Criteria	Sub-criteria	0	1	2	3	4	W	Σ
Report (4%)	English	Many sentences rendered nonsensical and many misspellings	Some sentences rendered nonsensical and a few misspellings	Sentences with poor grammar, written in first or second person, and a few misspellings	Good grammar, not written in third person. A few grammatical and spelling mistakes.	Written in third person. A few grammatical or spelling mistakes	1	/4
	Template	No structure followed	No numbering but structure present	Incorrect frontmatter or backmatter, but main matter correct structure. No figure, listing or table captions.	No citations or references, or incorrect bibliography style applied	Correct template, citations/references, numbering and template compliance.	1	/4

Business Network Archive: 2%

Criteria	Sub-criteria	0	1	2	3	4	W	Σ
BNA (2%)	Execution	Errors	Run-time errors	No errors (4)			1	/4
	BNA format	None	ACL	Node.js	CTO	Structure	1	/4

Lecture Aims

Aims

Apply and develop Access Control strategies for blockchain.

Lecture Objectives

Knowledge

- Implement Blockchain ACL
- Role-based access control
- Atribute based access control
- Apply different strategies of access control
- Control the authorisation of Participant's access to assets

Skills

Develop and implement access control for blockchain applications

Mandatory Access Control (MAC)

- Levels

MAC

Role-Based Access Control (RBAC)

- Academics, Students, Admin, Management, External
- All have different access to Systems
- M:N relationships between users and rights
- users cannot pass access permissions on to other users
- form of mandatory access control
- not multilevel

RBAC

A means of restricting access to objects based on the sensitivity of the information contained within the objects and the formal authorisation of subjects to access information of such sensitivity [**ferraiolo2001proposed**]

RBAC

- What is a Role?
- Set of transactions performed for access
- Transactions are allocated roles by SysAdmin
- Membership of a role
- Academics, Students, Admin, Management, External

Exam paper: Do's and Don'ts [mitchell:2019a]

- Module Leader writes exam paper.
- Internal moderator reviews exam paper.
- External Examiner checks process
- Module Leader responds
- Administrator signs-off
- Students complete exam

RBAC

- What is a Role?
- Set of transactions performed for access
- Transactions are allocated roles by SysAdmin
- Membership of a role
- Academics, Students, Admin, Management, External
- **Role Explosion**

Exam paper: Do's and Don'ts [mitchell:2019a]

- Module leader reviews submitted paper.
- Internal moderator submitting paper.
- External Examiner accessing incorrect papers
- Admin author paper
- Students views paper

Attribute-Based Access Control

- Protect objects
- Unauthorised operations
- ACL & RBAC
- Complex boolean rule set
- Rule set evaluates attribute
- Extensible Access Control Mark-up Language (XACML)

Attribute-Based Access Control

- Protect objects
- Unauthorised operations
- ACL & RBAC
- Complex boolean rule set
- Rule set evaluates attribute
- Extensible Access Control Mark-up Language (XACML)

Definition

An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions.
Vincent C. Hu *et al* [**huABAC**]

Attribute-Based Access Control

- Protect objects
- Unauthorised operations
- ACL & RBAC
- Complex boolean rule set
- Rule set evaluates attribute
- Extensible Access Control Mark-up Language (XACML)
- **Attributes**
- **Subject**
- **Object**
- **Operation**
- **Policy**
- **Environment**

Definition

An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions.
Vincent C. Hu *et al* [**huABAC**]

Hyperledger - Access Control Language

Review

- Permissioned blockchain
- Membership Services Provider (MSP)
- Fabric Certificate Authority (FCA)
- FCA issues Enrollment Certificates (e-certs)
- The e-cert is used as a signature
- user must register for e-cert
- Composer has BNA files
- Composer has cards

Attribute-based Access Control (ABAC)

- Fabric supports ABAC
- access control based on the attributes associated with the user identity
- Assets
- Participants
- Transactions
- Events
- Business Networks

  A business network is a collection of participants and assets that undergo a life cycle described by transactions. Events occur when transactions complete.

Access Control Language

Components

- Resources
  - namespace: org.example.*
  - namespace(recursive):org.example.**
  - Class in a ns: org.example.className
  - Instance of a class: org.example.className#ID
- operation
- participant
- transaction
- condition
- action

Access Control Language, ACL

Simple Rules

- Rules
- users
- permission
- create
- read
- update
- delete
- evaluated in order, first rule that matches is executed

Listing

```
rule ruleName {
  description:
  participant:
  operation:
  resource:
  action:
}
```

ACL

Simple Rules

Listing

```
rule ruleName {
  description:
  participant:
  operation:
  resource:
  action:
}
```