Selecting a Secure Cloud Provider: An Empirical Study and Multi Criteria Approach – Supplementary Material

Sebastian Pape, Federica Paci, Jan Jürjens, Fabio Massacci

1 Scenario Descriptions

1.1 Financial Services

You have to play the role of a tenant who would like to move to the cloud their infrastructure to deliver home banking and financial applications and data to their customers.

You have the following security requirements related to users' authentication and authorization:

- The cloud provider should support strong authentication mechanisms for critical services,applications and data
- The cloud provider should restrict access to critical services, applications and data only to authorised users
- The cloud provider should provide the ability to log access to critical services, applications and data
- The cloud provider should prevent the execution of malicious code

1.2 eCommerce

You have to play the role of a tenant (e.g online retailer) who would like to move to the cloud their IT infrastructure to run your online store.

You have the following security requirements:

- The cloud provider should protect the confidentiality of data during transport and at rest
- The cloud provider should maintain a vulnerability management program
- The cloud provider should support a strong access control mechanism
- The cloud provider should regularly monitor and test networks

1.3 eHealth

You have to play the role of a tenant (e.g healthcare organisation) who would like to move to the cloud their IT infrastructure to deliver clinical applications and data to their patient.

You have the following security requirements:

- The cloud provider should protect the confidentiality of data during transport and at rest
- The cloud provider should protect the privacy of the clinical data
- The cloud provider should protect the integrity of data during transport and at rest
- The cloud provider should guarantee the availability of clinical applications and data

2 Material Provided to the Participants

2.1 Financial Services

ID: S1C1A

First Name: ______________________

Last Name: ______________________

Start Time: ___:___

End Time: ___:___

Financial Services

You have to play the role of a tenant who would like to move to the cloud their infrastructure to deliver **home banking** and **financial** applications and data to their customers.

You have the following security requirements related to users' **authentication** and **authorization**:

1. The cloud provider should support strong authentication mechanisms for critical services, applications and data.
2. The cloud provider should restrict access to critical services, applications and data only to authorized users.
3. The cloud provider should provide the ability to log access to critical services, applications and data
4. The cloud provider should prevent the execution of malicious code

Post-Task Questionnaire:

http://www.surveygizmo.com/s3/1931194/cloud-post-A

(a) Scenario Description

No.	Question	Cloud Service Provider A	Cloud Service Provider B
1	Do you have a capability to use system geographic location as an authentication factor?	Yes	No
2	Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification?	Yes	Yes
3	Do you have controls in place ensuring timely removal of systems access which is no longer required for business purposes?	Yes	Yes
4	Do you document how you grant and approve access to tenant data?	NA	Yes
5	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	Yes	No
6	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or third parties?	Yes	Yes
7	Is any change in status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	Yes	Yes
8	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	Yes	Yes
9	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	Yes	Yes
10	Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	Yes	No
11	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	NA	Yes
12	Do you have anti-malware programs installed on all systems which support your cloud service offerings?	NA	Yes
13	Do you ensure that security threat detection systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted timeframes?	NA	Yes
14	Do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	Yes	Yes
15	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	Yes	Yes
16	Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?	Yes	Yes
17	Do you have an identity management system in place which enables both role-based and context-based entitlement to data (enables classification of data for a tenant)?	No	No
18	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometric, etc..) for user access?	Yes	No
19	Do you allow tenants to use third party identity assurance services?	Yes	No
20	Is Physical and logical user access to audit logs restricted to authorized personnel?	NA	Yes

Financial Services C1A

(b) Answers without Comments

No.	Question	Cloud Service Provider A (Answer)	Cloud Service Provider A (Comment)	Cloud Service Provider B (Answer)	Cloud Service Provider B (Comment)
1	Do you have a capability to use system geographic location as an authentication factor?	Yes		No	No. CSP B does not currently have the ability support GeoIP, but can support limiting access to specific IP addresses and ranges.
2	Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification?	Yes		Yes	
3	Do you have controls in place ensuring timely removal of systems access which is no longer required for business purposes?	Yes		Yes	
4	Do you document how you grant and approve access to tenant data?	NA	SDSU will be on private secure cloud.	Yes	
5	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	Yes		No	
6	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or third parties?	Yes		Yes	Administrative functionality is provided to customers to immediately revoke user access to CSP B.
7	Is any change in status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	Yes		Yes	Yes, administrative functionality is provided to customers to immediately revoke user access to CSP B.
8	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	Yes		Yes	
9	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	Yes		Yes	
10	Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	Yes	However, an NDA must be signed.	No	No, however, CSP B's security and access controls are designed to limit administrator functionality to enabling/disabling users. By design, administrators have no access to tenant data created or managed by any other user.

Financial Services C1B

(c) Answers with Comments, Page 1

No.	Question	Cloud Service Provider A (Answer)	Cloud Service Provider A (Comment)	Cloud Service Provider B (Answer)	Cloud Service Provider B (Comment)
11	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	NA	This question is specific to a public cloud solution.	Yes	Yes, CSP B maintains roles within the application that customers can utilize to fulfill their SoD requirements.
12	Do you have anti-malware programs installed on all systems which support your cloud service offerings?	NA	This is for public not private cloud	Yes	
13	Do you ensure that security threat detection systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted timeframes?	NA	This is for public not private cloud	Yes	
14	Do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	Yes		Yes	
15	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	Yes		Yes	
16	Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?	Yes		Yes	
17	Do you have an identity management system in place which enables both role-based and context-based entitlement to data (enables classification of data for a tenant)?	No		No	Planned.
18	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometric, etc..) for user access?	Yes		No	Planned.
19	Do you allow tenants to use third party identity assurance services?	Yes		No	
20	Is Physical and logical user access to audit logs restricted to authorized personnel?	NA		Yes	

Financial Services C1B

(d) Answers with Comments, Page 2

Figure 1: Experiment 1 on Financial Services

2.2 eCommerce

ID: S1C2A

First Name: _____

Last Name: _____

Start Time: ___:___

End Time: ___:___

eCommerce Services

You have to play the role of a tenant (e.g online retailer) who would like to move to the cloud their IT infrastructure to run your **online store**.

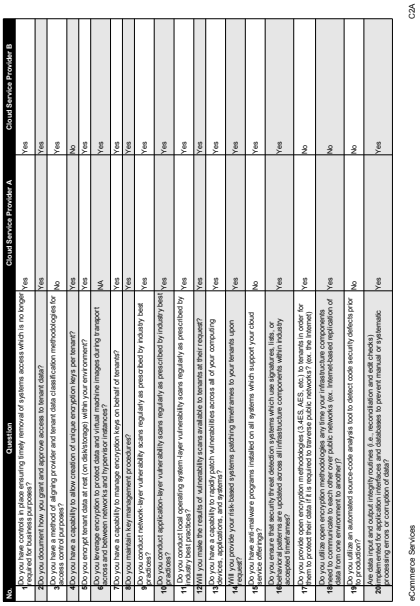
You have the following security requirements:

1. The cloud provider should protect the confidentiality of data during transport and at rest
2. The cloud provider should maintain a vulnerability management program
3. The cloud provider should support a strong access control mechanism
4. The cloud provider should regularly monitor and test networks

Post-Task Questionnaire:

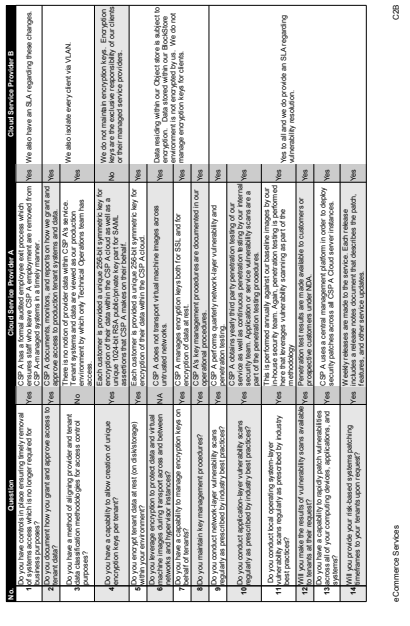
http://www.surveygizmo.com/s3/1931194/cloud-post-A

(a) Scenario Description



No.	Question	Cloud Service Provider A	Cloud Service Provider B
1	Do you have controls in place ensuring timely removal of systems access which is no longer required for business purposes?	Yes	Yes
2	Do you document how you grant and approve access to tenant data?	Yes	Yes
3	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	No	Yes
4	Do you have a capability to allow creation of unique encryption keys per tenant?	Yes	No
5	Do you encrypt tenant data at rest (on disk/storage) within your environment?	Yes	Yes
6	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	NA	Yes
7	Do you have a capability to manage encryption keys on behalf of tenants?	Yes	Yes
8	Do you maintain key management procedures?	Yes	Yes
9	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Yes	Yes
10	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	Yes	Yes
11	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	Yes	Yes
12	Will you make the results of vulnerability scans available to tenants at their request?	Yes	Yes
13	Do you patch your computing services, applications, and systems?	Yes	Yes
14	Will you provide your risk-based systems patching timeframes to your tenants upon request?	Yes	Yes

(b) Answers without Comments



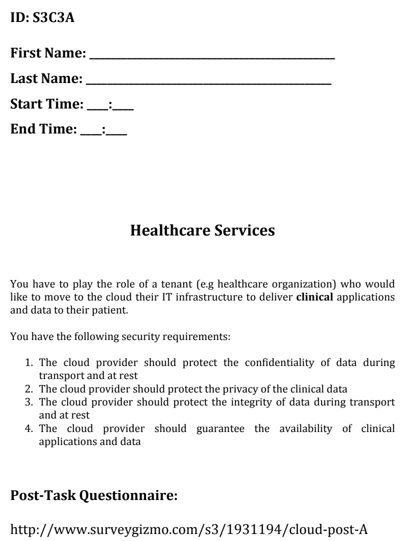
No.	Question	Cloud Service Provider A	Cloud Service Provider B
1	Do you have controls in place ensuring timely removal of systems access which is no longer required for business purposes?	Yes	Yes
2	Do you document how you grant and approve access to tenant data?	Yes	Yes
3	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	No	Yes
4	Do you have a capability to allow creation of unique encryption keys per tenant?	Yes	No
5	Do you encrypt tenant data at rest (on disk/storage) within your environment?	Yes	Yes
6	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	NA	Yes
7	Do you have a capability to manage encryption keys on behalf of tenants?	Yes	Yes
8	Do you maintain key management procedures?	Yes	Yes
9	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Yes	Yes
10	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	Yes	Yes
11	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	Yes	Yes
12	Will you make the results of vulnerability scans available to tenants at their request?	Yes	Yes
13	Do you patch your computing services, applications, and systems?	Yes	Yes
14	Will you provide your risk-based systems patching timeframes to your tenants upon request?	Yes	Yes
15	Do you have anti-malware programs installed on all systems which support your cloud service offerings?	Yes	No
16	Do you ensure that security threat detection systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted timeframes?	Yes	Yes
17	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to traverse public networks? (ex. the Internet)	Yes	No
18	Do you utilize open encryption methodologies any time your infrastructure components need to communicate to each other over public networks (ex. Internet-based replication of data from one environment to another)?	No	No
19	Do you utilize an automated source-code analysis tool to detect code security defects prior to production?	No	Yes
20	Are data input and output integrity routines (i.e. reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	Yes	Yes

(c) Answers with Comments, Page 1

(d) Answers with Comments, Page 2

Figure 2: Experiment 2 on eCommerce Services

2.3 eHealth



ID: S3C3A

First Name: ______________________________

Last Name: ______________________________

Start Time: ___:___

End Time: ___:___

Healthcare Services

You have to play the role of a tenant (e.g healthcare organization) who would like to move to the cloud their IT infrastructure to deliver **clinical** applications and data to their patient.

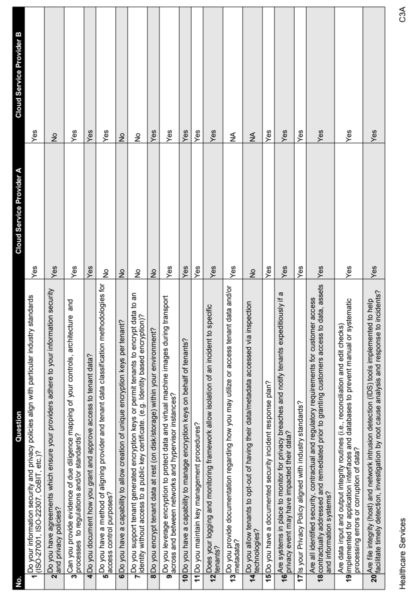
You have the following security requirements:

1. The cloud provider should protect the confidentiality of data during transport and at rest
2. The cloud provider should protect the privacy of the clinical data
3. The cloud provider should protect the integrity of data during transport and at rest
4. The cloud provider should guarantee the availability of clinical applications and data

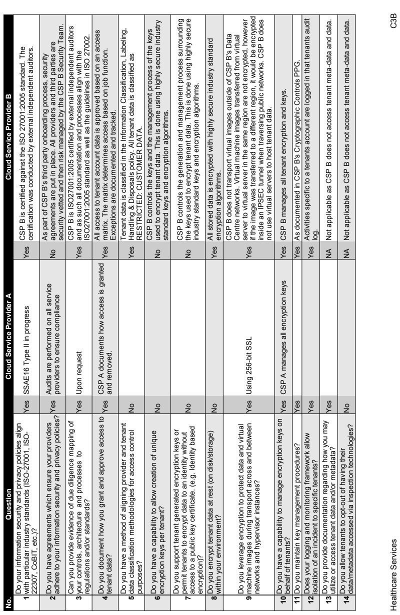
Post-Task Questionnaire:

http://www.surveygizmo.com/s3/1931194/cloud-post-A

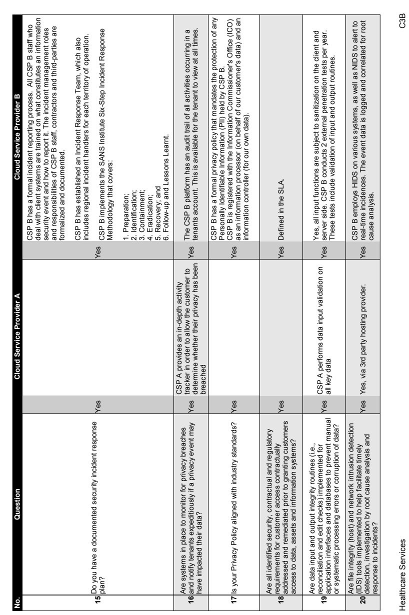
(a) Scenario Description



(b) Answers without Comments



(c) Answers with Comments, Page 1



(d) Answers with Comments, Page 2

Figure 3: Experiment 3 on Healthcare Services

3 Result of Our Approach

3.1 Financial Services

CSP	Choice	Access Control	Accountability	Insider Threat	Anti-Malware	Multifactor Auth.	Transparency	Result	Yes-Answers
1		0.0332	0.0423	0.0435	0.0418	0.0612	0.0157	0.0437	19
2		0.0435	0.0522	0.0177	0.0503	0.0326	0.0571	0.0417	18
3		0.0368	0.0522	0.0373	0.0084	0.0275	0.0571	0.0366	17
4		0.0326	0.0293	0.0373	0.0292	0.0488	0.0453	0.0366	20
5		0.0319	0.0293	0.0263	0.0292	0.0488	0.0350	0.0349	20
6		0.0319	0.0293	0.0263	0.0292	0.0488	0.0350	0.0349	20
7		0.0290	0.0423	0.0133	0.0503	0.0267	0.0207	0.0320	19
8		0.0315	0.0293	0.0263	0.0153	0.0434	0.0286	0.0318	19
9		0.0241	0.0293	0.0263	0.0292	0.0434	0.0350	0.0315	18
10		0.0426	0.0202	0.0339	0.0347	0.0273	0.0453	0.0315	20
11		0.0307	0.0293	0.0263	0.0292	0.0364	0.0350	0.0314	20
12		0.0319	0.0211	0.0263	0.0104	0.0434	0.0185	0.0289	17
13	A	0.0230	0.0253	0.0200	0.0037	0.0488	0.0133	0.0277	14
14		0.0277	0.0293	0.0339	0.0169	0.0265	0.0286	0.0274	20
15		0.0262	0.0215	0.0237	0.0292	0.0358	0.0195	0.0272	16
16		0.0208	0.0293	0.0237	0.0153	0.0366	0.0218	0.0268	15
17		0.0343	0.0143	0.0435	0.0503	0.0186	0.0135	0.0266	17
18		0.0221	0.0423	0.0184	0.0503	0.0104	0.0207	0.0265	17
19		0.0276	0.0045	0.0212	0.0169	0.0534	0.0178	0.0263	16
20		0.0310	0.0293	0.0263	0.0292	0.0125	0.0350	0.0254	18
21		0.0235	0.0293	0.0263	0.0292	0.0147	0.0350	0.0240	17
22		0.0216	0.0293	0.0263	0.0292	0.0155	0.0350	0.0237	14
23		0.0238	0.0293	0.0263	0.0292	0.0147	0.0218	0.0235	16
24		0.0263	0.0233	0.0263	0.0449	0.0133	0.0167	0.0235	17
25		0.0220	0.0233	0.0237	0.0449	0.0186	0.0167	0.0235	16
26		0.0301	0.0253	0.0263	0.0200	0.0125	0.0373	0.0234	18
27		0.0342	0.0163	0.0228	0.0039	0.0275	0.0146	0.0231	15
28		0.0227	0.0211	0.0237	0.0292	0.0234	0.0185	0.0230	14
29		0.0165	0.0423	0.0339	0.0254	0.0062	0.0157	0.0229	15
30		0.0239	0.0215	0.0263	0.0292	0.0186	0.0298	0.0229	16
31		0.0253	0.0293	0.0263	0.0153	0.0125	0.0350	0.0226	18
32		0.0148	0.0202	0.0177	0.0169	0.0366	0.0226	0.0226	12
33		0.0175	0.0293	0.0370	0.0208	0.0068	0.0453	0.0211	15
34	B	0.0233	0.0215	0.0263	0.0292	0.0102	0.0298	0.0206	14
35		0.0243	0.0117	0.0339	0.0169	0.0230	0.0115	0.0204	17
36		0.0179	0.0039	0.0228	0.0418	0.0099	0.0115	0.0147	12
37		0.0198	0.0211	0.0228	0.0048	0.0054	0.0053	0.0147	10

Table 1: Result for Experiment 1 on Financial Services

3.2 eCommerce

CSP	Choice	Anti-Malware	DP Rest	DP Transport	Key Management	Patching	Pentest	Transparency	Result	Yes-Answers
4		0.0292	0.0387	0.0477	0.0429	0.0255	0.0212	0.0395	0.0371	20
17		0.0503	0.0394	0.0341	0.0151	0.0404	0.0428	0.0143	0.0369	19
3	A	0.0084	0.0408	0.0311	0.0549	0.0474	0.0322	0.0318	0.0364	16
10		0.0347	0.0376	0.0343	0.0262	0.0474	0.0301	0.0449	0.0363	18
29		0.0254	0.0358	0.0338	0.0508	0.0197	0.0452	0.0630	0.0353	19
15		0.0292	0.0387	0.0319	0.0206	0.0255	0.0410	0.0115	0.0329	19
26		0.0200	0.0239	0.0410	0.0384	0.0255	0.0428	0.0395	0.0327	19
1		0.0418	0.0348	0.0283	0.0262	0.0415	0.0295	0.0160	0.0324	20
27		0.0039	0.0408	0.0311	0.0549	0.0415	0.0109	0.0230	0.0323	14
25		0.0449	0.0223	0.0477	0.0099	0.0232	0.0352	0.0160	0.0321	16
7		0.0503	0.0318	0.0367	0.0233	0.0138	0.0359	0.0230	0.0317	19
18		0.0503	0.0318	0.0374	0.0236	0.0138	0.0356	0.0160	0.0317	19
31		0.0153	0.0387	0.0299	0.0399	0.0255	0.0247	0.0395	0.0313	20
2		0.0503	0.0408	0.0117	0.0303	0.0474	0.0260	0.0318	0.0307	16
5		0.0292	0.0312	0.0283	0.0429	0.0255	0.0306	0.0395	0.0303	20
20		0.0292	0.0312	0.0283	0.0429	0.0255	0.0306	0.0395	0.0303	20
23		0.0292	0.0312	0.0283	0.0201	0.0255	0.0306	0.0395	0.0290	19
6		0.0292	0.0261	0.0283	0.0399	0.0255	0.0306	0.0395	0.0286	20
24		0.0449	0.0096	0.0477	0.0183	0.0232	0.0198	0.0230	0.0270	16
30		0.0292	0.0188	0.0341	0.0172	0.0232	0.0300	0.0230	0.0260	17
8		0.0153	0.0261	0.0213	0.0429	0.0255	0.0306	0.0395	0.0259	20
11		0.0292	0.0243	0.0208	0.0309	0.0255	0.0306	0.0395	0.0253	20
34		0.0292	0.0152	0.0341	0.0072	0.0232	0.0300	0.0230	0.0244	14
37		0.0048	0.0268	0.0283	0.0429	0.0209	0.0171	0.0057	0.0243	12
9		0.0292	0.0219	0.0239	0.0310	0.0255	0.0180	0.0395	0.0239	16
12		0.0104	0.0312	0.0183	0.0156	0.0255	0.0244	0.0395	0.0239	15
22		0.0292	0.0268	0.0283	0.0172	0.0118	0.0231	0.0074	0.0238	15
28		0.0292	0.0188	0.0208	0.0253	0.0255	0.0300	0.0264	0.0229	18
14	B	0.0169	0.0272	0.0113	0.0133	0.0474	0.0148	0.0318	0.0222	16
33		0.0208	0.0133	0.0216	0.0061	0.0474	0.0222	0.0248	0.0217	13
32		0.0169	0.0119	0.0307	0.0289	0.0209	0.0229	0.0057	0.0212	13
21		0.0292	0.0134	0.0179	0.0045	0.0255	0.0306	0.0395	0.0197	15
36		0.0418	0.0210	0.0224	0.0094	0.0114	0.0102	0.0044	0.0188	11
35		0.0169	0.0334	0.0056	0.0186	0.0138	0.0140	0.0080	0.0175	12
16		0.0153	0.0159	0.0060	0.0082	0.0221	0.0296	0.0143	0.0151	12
19		0.0169	0.0133	0.0050	0.0310	0.0209	0.0186	0.0327	0.0143	12
13		0.0037	0.0157	0.0121	0.0289	0.0208	0.0083	0.0044	0.0141	6

Table 2: Result for Experiment 2 on eCommerce Services

3.3 eHealth

CSP	Choice	Availability	Confidentiality	Integrity	Key Management	Privacy	Result	Yes-Asnwers
29		0.0286	0.0464	0.0526	0.0360	0.0266	0.0423	17
2		0.0232	0.0270	0.0508	0.0292	0.0265	0.0369	16
1		0.0451	0.0379	0.0250	0.0266	0.0460	0.0343	20
32		0.0451	0.0116	0.0381	0.0208	0.0302	0.0327	13
5		0.0249	0.0327	0.0346	0.0486	0.0294	0.0323	20
8		0.0249	0.0274	0.0346	0.0486	0.0326	0.0319	20
31		0.0353	0.0348	0.0250	0.0553	0.0364	0.0316	19
15		0.0249	0.0390	0.0346	0.0175	0.0255	0.0314	17
23		0.0249	0.0327	0.0346	0.0153	0.0294	0.0309	18
26		0.0249	0.0338	0.0346	0.0254	0.0252	0.0308	17
18		0.0451	0.0379	0.0250	0.0192	0.0249	0.0304	17
6		0.0249	0.0301	0.0346	0.0467	0.0202	0.0302	18
17	B	0.0451	0.0366	0.0250	0.0141	0.0221	0.0295	15
10		0.0451	0.0432	0.0130	0.0313	0.0410	0.0293	19
12		0.0249	0.0270	0.0346	0.0124	0.0255	0.0292	15
4		0.0347	0.0401	0.0215	0.0415	0.0268	0.0287	18
30		0.0249	0.0166	0.0346	0.0151	0.0319	0.0286	14
21		0.0249	0.0204	0.0346	0.0049	0.0294	0.0284	14
22		0.0205	0.0259	0.0346	0.0413	0.0163	0.0278	13
11		0.0189	0.0248	0.0326	0.0341	0.0259	0.0278	20
28		0.0249	0.0164	0.0346	0.0202	0.0255	0.0277	16
25		0.0189	0.0252	0.0326	0.0091	0.0289	0.0274	14
20		0.0126	0.0315	0.0305	0.0293	0.0280	0.0271	17
34		0.0249	0.0152	0.0346	0.0093	0.0248	0.0269	15
3		0.0286	0.0270	0.0195	0.0358	0.0377	0.0261	16
27		0.0224	0.0261	0.0174	0.0386	0.0430	0.0250	15
35		0.0286	0.0301	0.0195	0.0268	0.0272	0.0245	14
16		0.0249	0.0126	0.0346	0.0099	0.0133	0.0245	8
7		0.0242	0.0315	0.0180	0.0295	0.0320	0.0243	18
37		0.0121	0.0240	0.0303	0.0486	0.0141	0.0240	13
14		0.0134	0.0252	0.0176	0.0129	0.0376	0.0215	17
36		0.0451	0.0191	0.0120	0.0211	0.0240	0.0213	12
33		0.0451	0.0186	0.0130	0.0068	0.0184	0.0202	11
24	A	0.0189	0.0216	0.0135	0.0141	0.0302	0.0187	15
9		0.0249	0.0211	0.0085	0.0416	0.0294	0.0184	17
13		0.0121	0.0147	0.0042	0.0402	0.0072	0.0093	7
19		0.0073	0.0143	0.0051	0.0222	0.0071	0.0081	8

Table 3: Result for Experiment 3 on Healthcare Services