A Proposed Cloud Security Framework for Service Providers in Ghana

Richard Okoampa-Larbi
Presbyterian University
College, Ghana
Tema Campus

Frimpong Twum
(Corresponding author)
Department Of
Computer Science
Kwame Nkrumah
University of Science
and Technology,
Kumasi, Ghana

J. B. Hayfron-Acquah
Department Of
Computer Science
Kwame Nkrumah
University of Science
and Technology,
Kumasi, Ghana

ABSTRACT

The study proposes a cloud security framework for Cloud Service Providers (CSPs) in Ghana. It adopted a number of strategies, such as experimental research achieved through integrated simulation and mixed mode research method approach, using SPSS for data analysis to execute the study expectations of proposing a new cloud security framework. It also carried out an investigation into cloud security deployment technologies, and then undertook a comparative study of these technologies.

In addition, it also investigated whether or not CSPs in Ghana follow any cloud security policy guidelines to deliver cloud services in Ghana. An experimental research approach adopted an Open AM server for the purpose of achieving integrity and secure authorization in the proposed framework which employed XACML Version 3.0 to define and enforce policies. Tools such as, Cygwin, curl/libcurl, Scala and IntelliJ IDEA IDE were used together to enhance simulation in the study. The results from analysis revealed that, HSM, OTFE and other cloud based security systems are the major security technologies deployed by service providers for integrity and authorization. Two curl HTTP/ 1.1 GET request were made at the service application endpoint where the access controller is wrapped over. Based on the rule set, two basic users were allowed and disallowed when accessing a cloud resource. A basic resource of an application with HTTP gave a status and a security token. To maintain the integrity of cloud data, the study recommends a root hardware TPM Chip be adopted to ensure maximum application security and systems performance. The proposed security framework assures cloud data integrity and also ensures authorization. The study therefore also recommends XACML V 3.0 to be adopted as a language for cloud systems for policy definition and enforcement.

General Terms

Cloud security framework, Security technologies, Cloud Computing, Cloud service Providers in Ghana.

Keywords

Proposed Cloud security framework, Cloud Service, Service Providers in Ghana, Cloud security Policies, Cloud security technologies, Framework for Cloud security. CSP - Cloud Service Provider, DEK- Decryption Encryption Key, OTFE-On-The-Fly Encryption, TDE-Transparent Data Encryption, AC-Access Control, AP- Attribute Store, Policy Store, XACML-eXtensible Access Control Markup Language.

1. INTRODUCTION

Lots of benefits goes with the adoption of cloud computing despite the worrying trend of security issues. It has been known that one will not have to spend much on computing power, storage space and communication capacity from a large Cloud computing [1].

The issue of Privacy and the fear of information theft is on the rise. There are even at times when access to and control of data in the cloud becomes problematic. The problem could be that, technologies deployed by service providers for data protection does not provide a one-fit-all solution. The study investigates cloud security deployment technologies and goes further to know whether there or not there exist policy guidelines for CSPs in Ghana. One cannot omit the fact that, though there had been constant emergence of technologies, there is also no timely security standard developed for emerging technologies [2].

2. LITRATURE REVIEW

2.1 Technological Paradigms that led to Cloud Computing

Study has it that, the rapid growth and emergence of sophisticated communication technologies, the capacities in excess computing and again the changes in management philosophy are the three main factors that brought about cloud computing adoption [3]. However, others believe that, the origin of cloud computing services was as a result of continuous outdating of hardware and software resources[4].

2.2 Cloud Computing

Information is key to the growth of every organization. Trust, data privacy and access control contribute to the concerns raised about data protection. The National Institute of Standards and Technology (NIST) defined Cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Per the standards given by NIST, cloud computing is known for having five essential characteristics, three service models, and four deployment models [5]. There is however, the need to propose a more viable and a valid security framework for Cloud Service Providers, which will be based on a more robust and efficient security technologies and systems.

2.3 Cloud Computing Security Technologies

It is envisaged that, standards are made up of technologies in a framework. The several other security technologies reviewed in this work that depends on softwares are Open Authorization, Open ID, On The- Fly-Encryption, internet based softwaressuch as firewalls and on hardware are the Hardware Secure Module, Trusted Platform Module and XACML version 3.0 for access control in terms of policy definition and enforcement.In connection with the study also, Data Loss Prevention (DLP) strategy known to form part of encryption was one of the key data protection strategies that encompasses protection for endpoint DLP (data in use) and Network DLP (data in motion) [6].

2.4 Security frameworks and standards

The US Department of Homeland Security [7] defines a security standard as a technique, as policy, a procedure that attempt to protect the user's cyber environment. However, some experts are of the view that, there is no one-size-fits-all solution for cyber security [8].This preposition holds, in that bodies such asThe Cloud Security Alliance (CSA)continually provides technical updates on guidelinesfor the organization's information systems infrastructure. Aside what CSA provides, bodies such as, The United State National Institute of Standards and Technology (NIST), Institute of Electrical and Electronics Engineers (IEEE), European Network and Information Security Agency (ENISA)also provides theirown respective security standards which also covers the security aspect of an organizational IT systems[9]. The ISO/IEC 27001: 2013 for instance provides the requirement for Information security management systems. The ISO/IEC 27002: 2013 also provides the code of practice for information security controls. The standard depends on the processes adopted to build an information security management system [10]. The PCI DSS for instance was primarily developed to build and maintain network and systems, protect cardholder data, maintain a vulnerability management program, implement access control measures, regularly monitor and test networks and finally to maintain the information security policy [11].

2.4.1 Limitations of the reviewed frameworks

Among some of the limitations discovered during the review were, cost of security implementation, especially with reference to Payment Card Industry (PCI) Data Security Standard and Payment Application Data Security Standard (PCI DSS) of the version 3.0, implementation cost of security for cloud is expensive regarding expert or personnel, security systems and modules [11]. Again, Security sub components interdependency is one of the key issues. The components of the frameworks are large and complicated, and therefore lead to misinterpretation of prescriptions [12] [13]. Researchers are of the view that, objective Specification and Misinterpretation adds up to the numerous setbacks, because frameworks contain long list of compliances and specifications that can lead to misinterpretations [13].

2.5 Theoretical framework

The study adopted the Technology Acceptance Model (TAM) as suitable for testing the proposed framework. TAM stands out as a theory for measuring and determining individual's attitudes towards the acceptance and usage of a particular information system. In connection with this, [14] discussedTAM that the success of a system can be determined by a user's acceptance of the system which is usually measured by three main factors, such as perceived usefulness (PU), perceived ease of use (PEOU), and attitudes towards usage (ATU) of the system.

3. METHODOLOGY

The study employed a mixed mode research method approach and employed IBM's Statistical Package for Social Scientist (SPSS) version 21 to analyze data collected from the 12 sampled Cloud Service providing companies in Ghana using the purposive sampling technique. 5 questionnaires each were given out to each companies and at the end 60 respondents formed the entire population including IT managers, IT technical directors and the Cloud computing management team. The analysis was based on descriptive analysis and correlation. A proof of concept is used to simulate and approve the study resulting the proposed framework. In addition, an experimental research approach based on integrated simulation was employed. The tools and languages employed for the simulation were Open AM server, Cygwin, Curl/libcurl, Extensible Access Control Markup Language, XACML version 3.0, Scala programming language and IntelliJ IDEA IDE. The success was achieved through recording and reporting on results. During the simulation, a server application was developed in Scala and jyson; used to represent a cloud service platform application.Implementing the framework modularity, the endpoints of the server application is wired through the authorization server without the main server application being configured. A curl client is used to simulate a user agent (browser) request to the application. Two curl HTTP/ 1.1 GET request were made at the service application endpoint where the access controller is wrapped over. Upon request the secure controller accesses the Access Control List and verifies the payload. Upon verification, the payload is pushed to server for business. Though this approach can be seen as a single point of failure, the secure controller can be configured differently over many instance and also being highly scalable.

4. ANALYSIS, RESULTS AND DISCUSSIONS

4.1 Cloud security deployment technologies

Table 1: Which of the following cloud security technologies does your company depend on for data protection and maintaining the integrity of data?

Response	Frequency	Percentage
HSM	31	51.7
OTFE	29	48.3
Total	**60**	**100.0**

Source: Field data, 2016

Based on the questionnaire and the data analyzed, it was realized that 31(51.7%) of the respondents indicated HSM as a security technology in maintaining the integrity of the data whiles 29(48.3%) indicated using OTFE.

Table 2: Which of the following standardized authentication and authorization frameworks systems are deployed by your organization?

Response	Frequency	Percentage
SAML	18	30.0
SASL	12	20.0

OAuth 1	22	36.7
Others	8	13.3
Total	**60**	**100.0**

Source: Field data, 2016

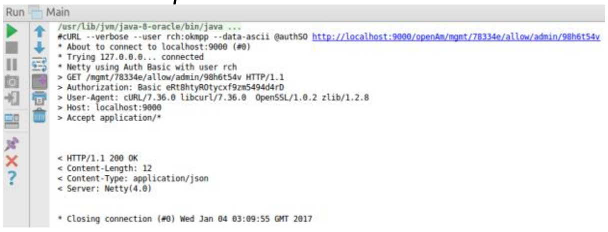
The responses of Table 2indicatethat the participating companieshave adopted authorization security frameworks standards such as SAML, SASL, and OAuth 1 although 8 of them stated others. ITU iterated in literature that[15], most African countries lack the accurate regulatory reference materials to provide cloud computing services. It was known that, majority of cloud providing companies have adopted policy guidelines in service provision. As revealed in the analysis, 44 (73.3%) depends on policy for service delivery whiles 16 (26.7%) does not. In addition, the analysis revealed that, quite a number adopts international policies for service delivery and data protection.

4.2 Correlations

As shown in Tables 3 and 4 above in this work, variables have no direct link with each other. This is because when the adoption of one variable increases the other decreases from time to time and vice versa. However, in correlating the various variables, the relationship between the various security techniques and strategies computed are all valid and significant at 1%. Cloud service providers adopts Internet softwares and other cloud security technologies such as HSM, OTFE, SAML, OAuth 1 for data protection**(see Table 3).** In addition, it was revealed that, at least one of the CSPs have deployed some of these cloud security technologies for protection. The idea is that the strategies were used simultaneously as shown for positive figures or correlations. From analysis, it means that when one technology is in use the other is neglected or abandoned by CSPs as represented for negative correlations or figures.

4.3 Proof of concept through simulation

4.3.1 Results from simulation



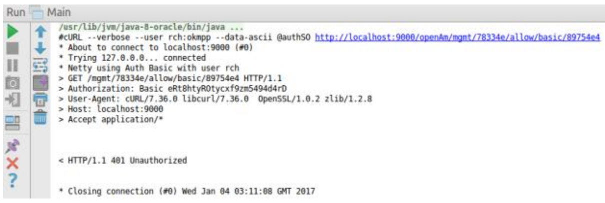
```
/usr/lib/jvm/java-8-oracle/bin/java ...
#cURL --verbose --user rch:okmpp --data-ascii @authSO http://localhost:9000/openAm/mgmt/78334e/allow/admin/98h6t54v
* About to connect to localhost:9000 (#0)
* Trying 127.0.0.0... connected
* Netty using Auth Basic with user rch
> GET /mgmt/78334e/allow/admin/98h6t54v HTTP/1.1
> Authorization: Basic eRt8htyROtycxf9zm5494d4rD
> User-Agent: cURL/7.36.0 libcurl/7.36.0  OpenSSL/1.0.2 zlib/1.2.8
> Host: localhost:9000
> Accept application/*


< HTTP/1.1 200 OK
< Content-Length: 12
< Content-Type: application/json
< Server: Netty(4.0)

* Closing connection (#0) Wed Jan 04 03:09:55 GMT 2017
```

Figure 1: Snapshot of Authorized client request from a server

cURL client receives an authorized response over a request to read a resource of id 23002. Authorization over HTTP response is 200 with basic token for subsequent authorization. The content type of the HTTP response is a text/plain which is the basic authorization token. Details of this are shown in the codes above.



```
/usr/lib/jvm/java-8-oracle/bin/java ...
#cURL --verbose --user rch:okmpp --data-ascii @authSO http://localhost:9000/openAm/mgmt/78334e/allow/basic/89754e4
* About to connect to localhost:9000 (#0)
* Trying 127.0.0.0... connected
* Netty using Auth Basic with user rch
> GET /mgmt/78334e/allow/basic/89754e4 HTTP/1.1
> Authorization: Basic eRt8htyROtycxf9zm5494d4rD
> User-Agent: cURL/7.36.0 libcurl/7.36.0  OpenSSL/1.0.2 zlib/1.2.8
> Host: localhost:9000
> Accept application/*


< HTTP/1.1 401 Unauthorized

* Closing connection (#0) Wed Jan 04 03:11:08 GMT 2017
```

Figure 2: Snapshot of Unauthorized request.

From the figure above **(see Figure 2)** a request was made from the Access Control server and the request/access denied, just as displayed with the HTTP/1.1 401.This is a cURL application interface tool integrated into Intellij IDEA IDE. This tool serves as a browser over HTTP 1.1 to query the URL with necessary (userID) data for client access to the system. cURL is used in lieu of a browser because cURL dumps all http client information in connection. Authorization code in the form of basic authorization is generated as a token for the user’s subsequent authorization. Client is unauthorized.

4.4 The Proposed Framework

The entire NIST framework meets five core expectations, that is, protect, response, detect, identify and recover in all cloud management operations [16]. It is therefore expected that the proposed framework below will provide a secure and fine-grained solution that resolves privacy and mitigate data control issues that may be encountered by CSPs in Ghana in the cloud system.

4.4.1 Deductions from the proposed framework

As at now the proposed framework**(see Figure 3)**cannot be fully implemented to function as stated. The proof of concept was performed to prove for validity and viability of the framework. This framework is service oriented and so, it is expected that the implementation of framework would exist in a modular architecture offering less component interdependency. The Access Control module as seen in the proposed framework must further be deployed into sub modules such as Authentication module and Authorization module. This makes it lightweight and less dependent modules.

Also, as shown in the diagram**(see Figure 3),** for the Private and the public networks, certain security systems and technologies, such as OTFE, HSM, DEK among the lots must not be confused with the other but rather be deployed specifically on those networks for proper management and monitoring. As seen, Service models (SaaS, PaaS, IaaS) are made available to the cloud consumers on their public network. But for higher security, security technologies such as HSM, OTFE, DEK Access Control systems must be deployed at the CSPs end for higher security. Hardware Secure Module (HSM) is an independent module that offers encryption management and encryption processes to the cloud system. HSM is a dedicated crypto processor that is specifically designed for the protection of the crypto key lifecycle. This is central or root to the framework and must be deployed on the private network of the Cloud Service Providers. Deploying HSM on private network ensures maximum security against external intrusion. Internal intrusion such as malicious insiders can further be restricted by assigning the HSM management to a particular host with human or biometric group factor authentication. Detriment to HSM is extremely unsafe. HSM manages Decryption and Encryption Keys [DEK], data encryption keys, data encryption processes, authentication, secure booting, digital signature generation and digital signing. Data center module as from the framework, represents the data storage component of the framework. Data management as specified earlier recommends the implementation of On-The-Fly Encryption-Transparent Data Encryption [OTFE - TDE] for improved performance and security. For a maximum security, it is recommended that the data center must be deployed on the private network for maximum security against both external and internal intrusions. Data center platform security, bootstrapping and [OTFE] is handled by HSM for optimum and central security. Data center OTFE helps in data loss prevention. Encrypted data loss can be classified as not data loss. Services models IaaS, PaaS and SaaS are deployed on the public network for external cloud consumers. A whole Private cloud deployment model may not need a public cloud feature. As such, the security of the public cloud lies on the private cloud. The private cloud of the CSP is recommended to host all security processes which cannot be accessed and breached on the public cloud.

4.4.2 Ensuring Integrity through a Hardware, TPM Chip.

Logically, it must be known that, the proposed framework will implement a Hardware Secure Module (HSM).It does employ Trusted Computing Group Trusted Platform Module (TPM) as a local root of trust of the system whiles the HSM by its performance provides the application software and utilities secondary encryption, authentication and signatures. The device, TPM, is a chip localized within the individual computer or server thus representing as a local HSM providing a perfect local root of trust for the system execution environment. The framework will depend on the root trust of a trusted hardware and that will help alleviates the effects of kernel mutability, that's the kernel fitting the needs of application, alterations of Virtual Machines cross attack or side channel attacks and even remote key injections. The essence of the TPM is to provide secured techniques such as secure boot, authenticated boot, public key based integrity checking. Thus, enhancing blind processing processes which is unseen by system administrators and users[17]. The integrity of a single hardware computer is achieved through the root hardware, TPM chip. However, using this approach performance suffers and hence an external HSM is attached to the system for application support and performance as shown in framework**(see Figure 3).**Virtual machine attacks, such as side channel or cross-attacks, could be reduced when a virtual TPM (vTPM) is introduced. Such attacks (Side channel), for instance occurs when a client on a virtual machine uses cryptographic keys of the Central Processing Unit (CPU) to access other virtual machines.

4.4.3 Reasons for framework adoption

Though there exist several frameworks, standards and technologies proposed by researchers and standard bodies, it is clearly evident that, the proposed framework in this work on evaluation,is capable of ensuring the following;

- Reducing cost of implementation and cost of management with high security efficiency and flexibility.
- Providing higher and flexible implementation of security of service and deployment models since security deployment can be modularized.
- Managing interdependency of security components for faster and efficient implementation thus providing efficient form of security for cloud computing systems.

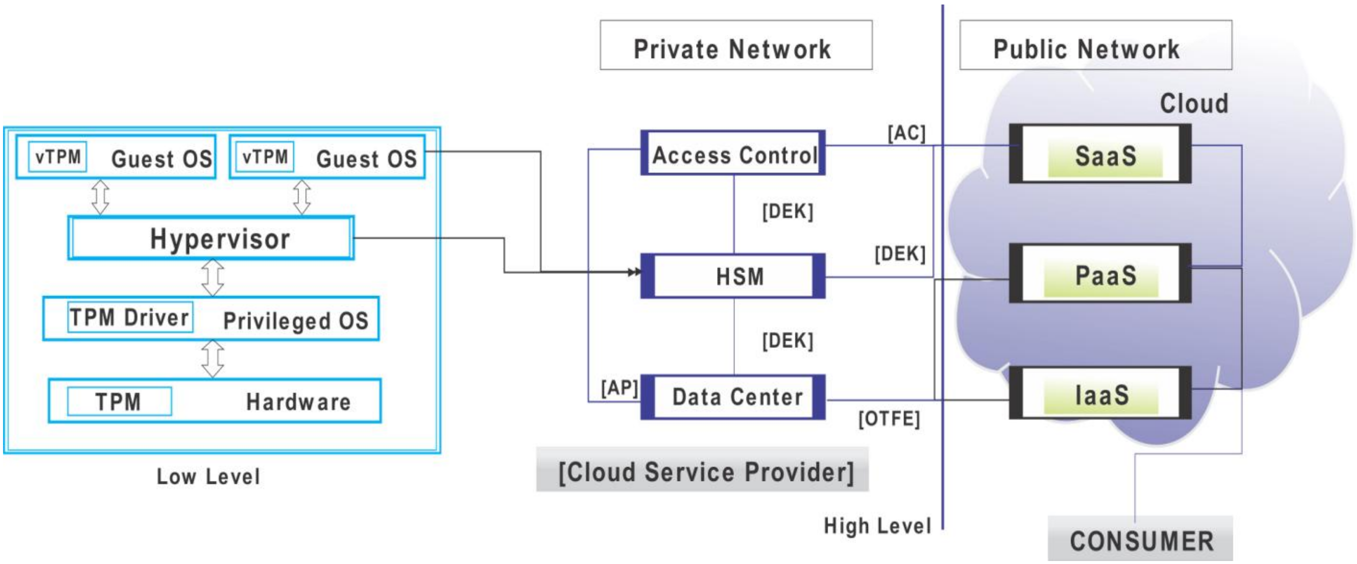


Figure 3: The Proposed data integrity and authorization Cloud Security Framework for Service Providers in Ghana

Source: (Authors Construct, 2016)

5. CONCLUSION

The study revealed that Cloud Service Providers (CSPs) are more comfortable adopting security technologies such as HSM, Internet softwares such as firewalls as the most appropriate ones for data protection. Therefore, to ensure the efficiency of the cloud system, security can be optimized by (CSPs) employing modules of the framework as native to the cloud system. With security implemented as a service, security adjustments and refactoring are fast and simple even in production. Data integrity through software means cannot only be a sure way for security and data protection but a more hopeful, thus, depending on the root trust hardware, called the TM Chip is potentially capable of reducing the bottlenecks.

In conclusion, it is a major struggle putting an end to cyber security threats [18]. This means that, all the confusion about security is based on trustof the cloud system.Therefore, in future, a more in-depth study into how the activities of consumers affect service providers' efficiency and service deliveryhas to be tackled.Not withholding the fact that, the proposed framework assuresexpected results, such as data integrity and secure authorization and recommended XACML version 3.0 as the best language for policy definition and enforcement.

6. ACKNOWLEDGMENTS

Many thanks to CSPs in Ghana and to my supervisor who played a key role in supervising this thesis.

7. REFERENCES

[1] Bisong, A., Rahman, M.S., 2011. An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011. DOI: 10.5121/ijnsa.2011.3103 30 from: http://airccse.org/journal/nsa/0111jnsa03.pdf ON 13th February,2015.

[2] Lewis, G.A., 2012. The Role of Standards in Cloud-Computing Interoperability. (October).

[3] Rajaraman, V., 2014. Cloud Computing. , (March), pp.242–258.

[4] Ramachandran, M., 2012. Service Component Architecture for building enterprise cloud services. Service technology magazine. Retrieved from http://www.servicetechmag.com/I65/0812-4 on 14th July, 2016.

[5] Mell, P. and Grance, T. 2011. The NIST definition of Cloud computing. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.

[6] Mogull, R. u.d. Best Practices for Endpoint Data Loss Prevention, Securosis, L.L.C.D. Sponsored by Symantec Inc.

[7] Department of Homeland Security, 2004, A Comparison of Cyber Security Standards Developed by the Oil and Gas Segment. (November 5, 2004).

[8] Price Water Cooperhouse, 2014.Why you should adopt the NIST Cyber security Framework. www.pwc.com/cybersecurity. May 2014

[9] Weiss, A., 2013. Cloud Security Standards: What You Should Know Retrieved from eSecurity Planet http://www.esecurityplanet.com/network-security/cloud-security-standards-what-you-should-know.html on 16th March, 2016.

[10] Brewer, D., 2013. Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013 The new international standard for information security management systems. BSI Group Information Security Management - Transition guide

[11] PCI Security Standards Council, 2013. Payment Card Industry (PCI) Data Security Standard. Summary of Changes from PCI DSS Version 2.0 to 3.0 Data Security Standard © 2006-2013, LLC. All Rights Reserved. Updated on November, 2013

[12] Indian Association of Extracorporeal Technology, IsecT, 2016

[13] Zeltser, L, 2016. Limitations of Frameworks in Information Security. Retrieved from htt1ps://zeltser.com/limitations-of-frameworks-in-infosec/ On 30 March, 2016.

[14] Davis, F. D., Bagozzi, R. P., and Warshaw, P. R., 1989. User acceptance of computer technology: A comparison of two theoretical model. Management Science, 35(8), 982-1003

[15] International Telecommunication Union, ITU, 2012. Cloud computing in Africa. Situation and perspective. Technology Development Centre. Regulatory & market environment

[16] National Institute of Standards for Technology, 2011.Cloud Computing Standards Roadmap, NIST CCSRWG– 070, Eleventh Working Draft, May 2, 2011 NIST Reference Architecture http://www.nist.gov/itl/cloud/refarch.cfm

[17] Naruchitparames, J. and Güneş, M.H., 2011, July. Enhancing data privacy and integrity in the cloud. In High Performance Computing and Simulation (HPCS), 2011 International Conference on (pp. 427-434). IEEE.

[18] McLellan, C. 2015. Cyber security in 2015: What to expect. Retrieved from

[19] http://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect/ on 14th July, 2016.

8. APPENDIX

Table 3: Do you receive training as service providers, either locally or internationally?

		Using internet based software	firewall	nothing	antivirus	other
Using internet based software	Pearson Correlation	1	-.966**	.^{b}	.^{b}	.^{b}
	Sig. (1-tailed)		.000	.	.	.
	N	60	60	60	60	60
firewall	Pearson Correlation	-.966**	1	.^{b}	.^{b}	.^{b}
	Sig. (1-tailed)	.000		.	.	.
	N	60	60	60	60	60
nothing	Pearson Correlation	.^{b}	.^{b}	.^{b}	.^{b}	.^{b}
	Sig. (1-tailed)	.	.		.	.
	N	60	60	60	60	60
antivirus	Pearson Correlation	.^{b}	.^{b}	.^{b}	.^{b}	.^{b}
	Sig. (1-tailed)	.	.	.		.
	N	60	60	60	60	60
other	Pearson Correlation	.^{b}	.^{b}	.^{b}	.^{b}	.^{b}
	Sig. (1-tailed)	.	.	.	.	
	N	60	60	60	60	60

Source: Field data, 2016 **correlation is significant at the 0.01 level (1-tailed)

T**able 4: Correlations between data protection security methods**

		encryption	secure socket	internal protocol	two factor	other
Encryption	Pearson Correlation	1	-1.000[**]	.[b]	.[b]	.[b]
	Sig. (2-tailed)		.000	.	.	.
	N	60	60	60	60	60
secure socket	Pearson Correlation	-1.000[**]	1	.[b]	.[b]	.[b]
	Sig. (2-tailed)	.000		.	.	.
	N	60	60	60	60	60
internal protocol	Pearson Correlation	.[b]	.[b]	.[b]	.[b]	.[b]
	Sig. (2-tailed)	.	.		.	.
	N	60	60	60	60	60
two factor	Pearson Correlation	.[b]	.[b]	.[b]	.[b]	.[b]
	Sig. (2-tailed)	.	.	.		.
	N	60	60	60	60	60
other	Pearson Correlation	.[b]	.[b]	.[b]	.[b]	.[b]
	Sig. (2-tailed)	.	.	.	.	
	N	60	60	60	60	60

Source: Field data, 2016 **. Correlation is significant at the 0.01 level (2-tailed).

b. Cannot be computed because at least one of the variables is constant.