Volume 4, Issue 10, October 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Study on Cryptography as a Service (CAAS)

Yudi Prayudi*, Tri K Priyambodo
Department of Informatics UII Yogyakarta Department of Computer Science and Electronics UGM Yogyakarta, Indonesia

Abstract*—Cloud is a solution that is offered to improve efficiency and service. Cryptography as a Service (CAAS) is included in one of the cloud services that are developed to provide a solution to the vulnerability that occurs on the endpoint cryptography process. CAAS is a strategic issue; cryptography is included in one of the dual-use technology, it is necessary to understand how it works properly. This paper is an exploration of the study provides CAAS issue through a comparison with the Kerberos protocol that has been widely known. The comparisons include the background, the ways of working, as well as the implementation of security. Although CAAS and Kerberos are two different things, it turns out both have the same function and purpose. CAAS serves to divert the cryptographic process on cloud services as a cryptographic security solution process on the endpoint device, while Kerberos is used to authenticate a user as the solution process of securing access to resources in a network. Both provide a security mechanism in the form of keeping something that is important (cryptographic keys, passwords) is not sent over the network but stored and processed in a separate machine.

***Keywords*— Cryptography, Authentication, Cloud, Kerberos, CAAS**

I. INTRODUCTION

In the last three decades, according to [1] there has been a shift in trend of computing that is from client-server to the distributed systems then centralized virtually known as cloud computing. In general, NIST defines cloud computing is a form of information technology services that is on-demand with a specific configuration, but can be quickly run over Internet networks. Issues of storage and infrastructure cost savings as well as efficiency have become an attraction for the customer to switch to utilizing cloud solutions [2]. On the other hand, the potential of a commercial market for cloud services, increasing from year to year would be a challenge for cloud service providers to provide a wide variety of services based on cloud computing. Therefore, cryptography as a service is presented as a cloud service solution to resolve the need for computer security.

Availability of cloud service providers for cryptographic services (cryptography as a Service-CAAS) is one of the issues that must be explored. Cryptography is included in the category of "dual use" technology, a technology that usage should be regulated because it can be employed for either commercial purposes or military purposes. If in the future it turns out that this technology will be readily available and offered by cloud service providers, then the efforts to monitor the use of cryptographic technology on society will be difficult eventually.

There are a number of models that serve as cryptographic application solutions in the cloud environment, as proposed by [3], [4], [5], [6]. One interesting thing that encourages researchers to conduct further studies is the CAAS model developed by Robinson [3], [5] and presented in RSA Conference in 2013 and 2014. In this case, according to [5] endpoint device are very prone to the vulnerability and seen as a bad place to produce key generator, but it is generally a cryptographic solution which naturally has been applied as an endpoint cryptography process, that is applying the encryption process and storing its cryptography keys on endpoint devices. This is because the new scheme of cryptographic implementation is proposed by preparing CAAS providers to help endpoint devices running the cryptographic operations via the web services without exposing its key to the endpoint device.

The proposed CAAS model has the potential to apply because it provides a solution for cryptographic needs on a variety of mobile devices that usage is increasingly widespread in the community. Unfortunately, there is not much information that can be extracted about the CAAS models except what is conveyed in the presentation document of the RSA Conference in 2013 and 2014. In an effort to explore further understanding about this CAAS, what can be done is to do a comparison with certain models that are more understood by the public. In this case, the Kerberos protocol is chosen as a model to make comparisons considering that the Kerberos protocol has existed quite long and widely known. By observing the CAAS model and its analogy with the workings of the Kerberos protocol, it is expected to be able to understand the CAAS models, explore it further and then take further advantage of the opportunities and challenges of research on the CAAS issue.

This paper is a literature study by utilizing the resources available on the internet that discuss the issues of CAAS and Kerberos. In the next section of this paper will discuss about the evolving terminology CAAS, the CAAS model proposed by Robinson, basic principles of the Kerberos protocol, the deepening of CAAS through Kerberos protocol comparison and the final conclusion in the form of a general overview of CAAS as well as the suggestions for the next research.

II. TERMINOLOGY OF CAAS

A. General Terminology

Terminology of CAAS is still relatively new, so there are differences on the views between one researcher and other researchers as well as among computer security industry practitioners.Several definitions and applications of terminology of CAAS publicized in a number of papers are:

a. CAAS as *Communications as a Service.* This terminology is proposed by [8], which is a service that includes: dedicated bandwidth, network security, encryption and network monitoring.
b. CAAS as *Cryptography as a Service.* This terminology is proposed by a number of researchers, who are: ([3], [4], [5], [6]. The point is to discuss computer security solutions in the cloud computing scheme.
c. CAAS as *Confidentiality as a Service.* This terminology is presented by [9]. This service is a solution to the need to maintain the confidentiality and integrity of critical data stored in various cloud services.
d. Similar issue with the CAAS is *Encription as a Service* (EaaS) proposed by [6] and *the Security as a Service* (SecaaS) proposed by [10]. Both termstend to define how to provide security solutions on the cloud provider primarily through cloud system architecture approach.

This paper will focus on the term of CAAS as Cryptography as a Service, although in some aspects, it almost has the same meaning with Encryption as a Service (EaaS) or Security as a Service (SecaaS).

B. CAAS as Crptography as a Service

CAAS as Cryptography as a Servicestill has the differences in meaning between one researcher and another, which generally there are three meanings that can be inferred to explain Cryptography as a Service.

a. Cryptography Solutions for Cloud Computing Services. The focus is on how to improve the *degree of trust* of the cloud usersto be*acceptable levels* [11]. There is the concept of *Self-Authentication Key* method of [3], concept of *cloud architecture*of [11] and [4].
b. Cryptographic Processes through Service Provider. It is proposed by [5], thatis a new mechanism so that cryptographic keys are no longer needed on theendpoint, but kept in a separate place;still, it does not decrease the performance of an existing web service. CAAS is a solution for strong cryptographic service availability without having to use the help of the Hardware Security Module (HSM) or a crypto processor.
c. HSM SolutionstoCryptography. The solution is in the form of a virtualHardware Security Module (HSM)service provision. One example of a vendor for this service is Cryptomathics and SafeNet Crypto Hypervisor.

The difference meaning is due to the different perspectives in looking at the problems and cryptographic solutions on the cloud. The first viewpoint is viewing the cloud as a service and infrastructure which must be supported by a good cryptographic technology so that all data and processes in the cloud are completely protected. Meanwhile,the second viewpoint is how to run a cryptographic function through cloud services. If the expectations of the service of Cryptograhy as a Service (CAAS) is a cloud services to help the users in overcoming cryptographic issues for various operated applications or business models, the meaning proposed by [5], [7] is the relevant one.

III. BASIC PRINCIPLE OF CRYPTOGRAPHY AS A SERVICE

A. The Background of CAAS

According to [5], putting the cryptographic keys on the endpoint devices such as smartphones and public cloud services will pose its own risks. These equipments generally apply endpoint cryptography and are very susceptible to the vulnerability and seen as a bad place to generate a key generator. The application of cryptography on each endpoint deviceshas a lot of vulnerability risks such as: the risk of theft of key data due to loss of endpoint devices,data theft because of illegal backups or malware that performs the function of data theft. It indicates that the equipment is not safe to store cryptographic keys. This is what underlies [5], [7] to propose a new scheme of CAAS that will provide functions of:

- preparing the CAAS providers to help endpoint devices running cryptographic operations via the web services without exposing the key to the endpoint devices*;*
- improving the quality of cryptographic keys for endpoint devices through the use of entropy on the endpoint devices;

General description of the process is presented in Figure 1. With the various advantages and disadvantages, CAAS is actually expected to be a solution for strong cryptographic service availability without having to use the help of the Hardware Security Module (HSM) or a crypto processor.

Figure 1 The Problems and Solutions of Endpoint Cryptography Process
(Picture taken from Robinson [5],[7])

B. How CAAS Works

CAAS model proposed by [5], [7] is a mechanism of"cryptographic operations on behalf of endpoints via web services". This can be explained as illustrated in Figure 2. Based on the illustration, forthe implementation of CAAS on the smartphone application email delivery, its steps are as follows:

1. Log in theapplication on the *endpoint* device.
2. Strong authentification process between *endpoints*and CAASservice.
3. If it issuccessful, then authentification token is obtained.
4. Users write email content that will be sent.
5. Plain Text email and authentification token are sent to the service provider.
6. The output is a signed email.
7. Signed email is then sent by an endpoint to the email server.

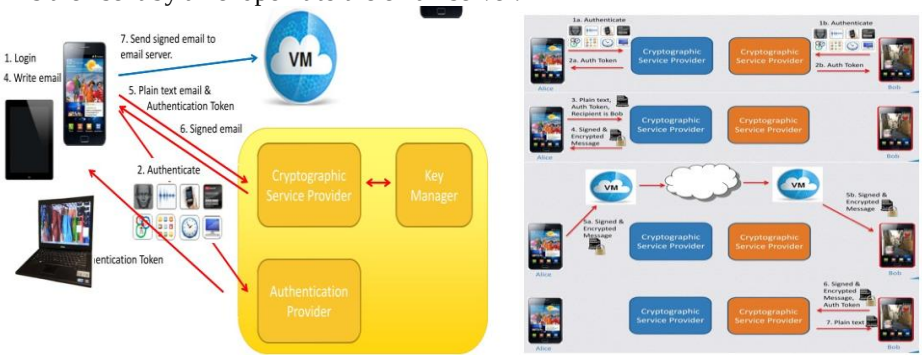

Figure 2 Illustration ofHow CAAS Works
(Picture taken from Robinson [5],[7])

According to [7], CAAS services only require endpoi*nt* deviceauthentication to ensure that the device is able to perform access to CAAS. Therefore,a strict mechanism is needed to authenticate (strong authentication*)*.This process can be done through a user authentication (passwords, voice, facial recognition, motion-based, one-time password*)* and the environmental authentication (Device ID, driver's license number, phone number, MAC Address, Location, Apps allowed to be on the phone, Time of day).

All operations to generate a cryptographic key are run by the CAAS provider through a Representational StateTransfer (REST) or Key Management Interoperability Protocol (FOI) that run over Transport Layer Security (TLS). Through this solution, the endpoint devices (for example, mobile phones) do not need to keep the key in the cell phone but are still able to send and receive encrypted messages, see the encrypted data in the handphone as well as see the encrypted data in the cloud.

C. Implementation of CAAS

CAAS may be applied, among others, for the benefit of the e-mail application use, seeing the encrypted data stored on the endpoint or on the cloud and performing sharing between devices. In terms of using an email application, the owner of an endpoint device can send signed email and receive encrypted messages through the mechanism of CAAS. The illustration of its application is presented in Figure 2.

D. Security Issues

CAAS Service still has not been fully tested yet especiallyto overcome networking issues, for example, when endpoint devices cannot connect to the CAAS provider, and also security issues about the cache that stores important keys and information about user authentication. In terms of cloud services in general, it still remains a challenge regarding the safety, even though ituses the private cloud solution. Another security challenge for the CAAS is how to maintain communication between endpoints and CAAS Provider which is always ina trustworthy scheme. If an attacker successfully masters the endpoint device and passes the authentication of service provider, then all the available services can be mastered.

Related to the security of cloud computing, security experts are still in doubt on the reliability of security in cloud services. One of them is Ralph Spencer Poore, as reported by [12]. According to him, the cryptography matters and its security arehomeworks and it is advisable not to be complacent by all the imagination about cloud service solutions. Cryptographic problems are problems that are to be handled by self and are not included in the section that must be submitted to the other party (outsourcing). Cloud services tend to be transnational in nature, while cryptographic technology itself in a number of countries is a technology protected by law with a number of limited access and use. This aspect should be thoroughly understood by cloud service users and should have been included in the SLA (Service Level Agreement) provisions agreed in the contract.

IV. THE BASIC PRINCIPLE OF KERBEROS PROTOCOL

A. The Backgroud Of Kerberos

In a computer network, the application should only focus on providing services in accordance with its primary function. An example of such is the email service application; this application should focus on providing the best service

for sending an email, in fact similar application should also perform user verification process as well for the security of the mail delivery. It is then given by Kerberos; through this protocol, the processes associated with user authentication is handled entirely by the Kerberos so that the applications can focus on its tasks and services [13]

Kerberos is a cryptography-based authentication protocol in open network computing environments. This protocol is part of a system built under Project Athena developed by MIT. This protocol is named Kerberos, because Kerberos (or Cerberus) refers to the name of a Greek mythological three-headed dog that becomes the guard of Tartarus, a gateway to Hades (the story in the Roman-Greek mythology). Since its first publishingin 1983,Kerberos has now reached version 5.12.1 released in January 2014 [14]

There are four security aspects that must be considered in a network, namely: Authentication, Integrity, Confidentiality and Authorization. Authentication is a matter associated with the identity verification of a particular party; Integrity is a matter related to the data condition where the received data is the same as the produced/delivered data. Confidentiality is a matter related to the protection of provided information, so that it does not fall to other party which is not entitled.Meanwhile, Authorizationis the process of giving authority to those who are alreadyauthenticated to perform the operations that become its rights and authority.

In this case, Kerberos is a network protocol that handles the authentication issue. Kerberos is the authentication mechanism that is intended for a distributed server. It allows the servers and clients to perform mutual authentication process before making connections. The authentication process is a mechanism to validate the identity of the communication opponent. Such mechanism is one of important partsin network security. Without authentication, the party which has no right cannot access the confidential and important resource.

In its implementation, Kerberos is the default authentication method which is applied to Windows 2000 and Windows XP. There are two reasons why it was chosen by Windows. The first is because Kerberos has been proven as a powerful network authentication method and the second is because it is open source, so it allows Microsoft to add this Kerberos on itsdeveloped application [15].

B. How Kerberos Works

There are three sub-protocols of Kerberos, namely:

- Authentication Service (AS) Exchange: used by the Key Distribution Center (KDC) to provide the Ticket-Granting Ticket (TGT) to the client and create a logon session key.
- Ticket-Granting Service (TGS) Exchange: used by the KDC to distribute a session key services and tickets associated with it.
- Client/Server (CS) Exchange: used by the client to submit a registration to the ticket as registration to a service.

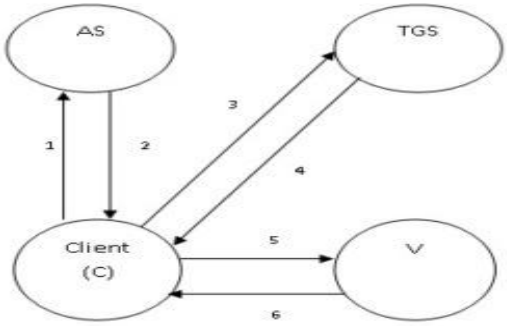

Figure 3 Overview of How Kerberos Works
(Picture taken from [13])

According to [13], in general, there are six stages of Kerberos architecture, namely:

1. Request for Ticket-Granting-Ticket. User personal informationis entered into the Kerberos client computer and then the computer will send a request to the KDC to access TGS by using the AS Exchange protocol. In the request, there is proof of user identity that has been encrypted.
2. Ticket-Granting-Ticket + Session Key. KDC receives a request from a Kerberos client, and then finds the primary key (called a Master Key) owned by the user in the directory service of Active Directory. Furthermore, it decrypts the identity information contained in the sent request. If the user identity is verified successfully, KDC will respond by giving TGT and a session key by using the US Exchange protocol.
3. Request for Service Granting Ticket. The client then sends a TGS request to the KDC containing TGT previously received from the KDC and request access on some services in the server by using the TGS Exchange protocol.
4. Service-Granting-Ticket + Session Key. The KDC then receives the request, authenticates the user, and responds by giving a ticket and session key for the user to access the target server by using the TGS Exchange protocol.
5. Request Service. Further, the client sends a request to the target server containing ticket previously obtained by using the CS Exchange protocol.
6. Provide Service Authentication Meaning. Target server authenticates the ticket in question, responds with a session key, and then the client is finally able to access the services available in the server.

Although the process looks complicated, but the work is conducted behind the scenes, so it is not visible to the user.

C. Implementation Of Kerberos

Authentication is the process in order to validate the user upon entering the system. The name and password of a user will be checked through the list showing those who havegiven the right to enter the system. This process is set-up by the administrator, webmaster or site owner (holder of the highest privileges or those designated in the system). According to [16], the authentication process is a mechanism to validate the identity of the communication opponent. This mechanism is one of the important parts of security network. Without the authentication, the party does not have the right to access confidential and important resource.

According to [14], Kerberos is designed both to facilitate the key distribution andto restrict the communication between users and servers. The goal is to allow the user and service to mutually authenticate each other;in other words, each show their identity. Actually, there are many ways to show the user's identity to the service, but the most common one is the use of passwords. In this case, the authentication process occurs when someone logs on to the server by typing a username and password, which is ideally known only by the user and the server. After that, the server is assured that the person trying to access is completelytheuser.

Kerberos is widely applied as a tool for the authentication process of interactive services, such as telnet, ftp, pop and so on where the users are prompted to enter a password to log in real time. Symmetry key allows that the authentication can be performed in real time because of its rapid characteristic. Symmetric key algorithms use the same key for encryption and decryption.

In principle, Kerberos can be used as a solution for user authentication both for single-platform and multi-platform. Kerberos is the authentication mechanism intended for distributed server; this allows the server and client to authenticate each other before making the connection. IBM itself provides a commercial version of Kerberos in the form of Global Sign On (GSO) application.

D. Security Issues of Kerberos

Security elements in a network are very important to note. One important aspect of network security is the authentication mechanism. One of the protocols that can be used for authentication mechanism is Kerberos, which is now up to version 5. Kerberos authentication system is one of the solutions to overcome the security attacks on the network which becomes the weakness of conventional authentication system (password-based).

Authentication mechanism by Kerberos is carried out by using a shared private key between the client and the server. The private key is issued by a trusted third party. Username and password of client which are not sent over the network is one of the advantages of the Kerberos authentication system. The use of sesssion key is also able to enhance the communication security with the Kerberos protocol.

According to [13], two of the Kerberos security issuesareabout Replay attack and password. Kerberos uses the time-stamp to determine whether the authenticatorsent is new (not a replay attack). Therefore, time synchronization over the network is required. In this case, a lot of things have been proposed to resolve the solution to both issues, but generally the proposed solution impactson an increase in the complexity of Kerberos. Therefore, other solution proposed by [13] is using Triple Password Schema. Another opinion about Kerberos security issue, according to [16] is its inability to handle an attacker yet who performspassword guessing.

V. DISCUSSION

Based on the previous description, it seems that the main issue of CAAS is about the endpointcryptography,since putting cryptographic keys on endpoint devices will pose its own risks and is very susceptible to the vulnerability. In this issue, theendpointdevice is seen as a bad place to generate key generator. The solution is to prepare providers to help endpoint devices run the cryptographic operations via the web services without exposing the key to end-point devices. Meanwhile, Kerberos is developed as a solution to overcome the security attacks on network which becomes the weakness of conventional authentication system (password-based). The goal is to allow the user and service to mutually authenticate each other.

Both CAAS and Kerberos actually have the same function that is to provide access to a number of resources/applications; nevertheless, both are just different in shape. CAAS provides access to the resource through the process of encryption and decryption of cryptographic keys used to secure the service, while Kerberos provides access to resources through the granting ticket mechanism. Both CAAS and Kerberos provide a mechanism whereimportant things (Cryptography key or username, passwords) are not sent over the network but ratherperformed on computer machine itself. In this case, the machines used to perform the functions of CAAS are: Endpoint device, Cryptograhy Service Provider, User Authentication Providers and Key Manager. Meanwhile,the machines used to run the Kerberos functions are: Client, Server and ServerKerberos-Key Data Center (KDC).

From the aspect of implementation, the CAAS solution proposed by Robinson is still not reviewed yet, investigated further, or even implemented directly. Of course, this is in contrast to Kerberos which has been widely adopted and implemented by numerous vendors for various uses of user authentication mechanism. However, the CAAS solution is very interesting considering the fact that the number of mobile device users and the availability of a wide range of applications on the platform are largerand more varied. Thus, the CAAS solution is actually a very strategic one.

From the security aspect, CAAS concept relies heavily on a mechanisms to ensure that the owner of the endpoint device is actually the legal owner of the device, so that the person has the authority to access the application. To support this, the proposed mechanism is using strong authentication on end-point devices.

Especially for the availability of cloud services, the implementation of CAAS remains to be seen further based on mechanism for the implementation of cryptographic technology as the main service of its cloud. Legal and jurisdiction issues of the implementation are matters that have not been studied further yet. From the infrastructure aspect, the implementation of hardware security module machine on its cryptographic machine as well as the trusted computing concept underlyingit is still a topic that needs to be studied further. In addition, one issue that still needs to be explored is about utilizing the Transport Layer Security (TLS) used as a medium for communication between providers and an endpoint.

Table 1 Comparison of CAAS and Kerberos

No.	The element	CAAS	Kerberos
1	Keyword	"cryptographic operations on behalf of endpoints via web services"	Solutions for user authentication
2	Input→Output	Strong Authentication→cryptographic keys to run or access the application/resource.	Password, Username→ access permissions to the resource
4	The Primary Machine	Endpoint, Cryptograhy Service Provider, User Authentication Provider, Key Manager	Client, Server and server Kerberos (KDC) with three sub-protocols: the Authentication Service (AS) Exchange, Ticket-Granting Service (TGS) Exchange, Client/Server (CS) Exchange.
5	Background	• The risks of vulnerability to the implementation ofendpoint cryptography. • Preparing providers to help endpoint devices run the cryptographic operations via the web services without exposing the key to the endpointdevice.	• The weakness of conventional authentication system (password-based). • Setting up a mechanism that allows the user and service to mutually authenticate each other.
6	Working Principle	Endpoint devices do not need to store cryptographic keys, cryptographic processes and its key storage arecarried out on the server cloud. It uses strong authentication for endpoint devices.	No password or a secret key in the form of plaintext is sent over the network. The secret key is only used locally to decrypt the ticket.
7	Implementation	It is still at the level of the concept, but the principle of CAAS can be used for the benefit of sending signed email and receiving encrypted messages. Seeing the encrypted data stored on the endpoint or on the cloud. Performing sharing between devices.	Kerberos is widely applied as a tool for the authentication process of interactive services, such as telnet, ftp, pop.

VI. CONCLUSION AND SUGGESTION

Based on this analysis, it can be seen that although the CAAS and Kerberos are two different objects, actually theyhavesimilarity in its functions and ways of working. CAAS focuses on providing cryptographic services based on the cloud, while Kerberos is a protocol for authenticating users in a computer network.

On CAAS, all processes are carried out with the support of endpoint devices, Cryptograhy Service Provider, User Authentication Provider and Key Manager through a strong user authentication mechanism. While on the Kerberos, all processes run through the Client, Server and Server Kerberos (KDC) with the support of three sub-protocols: the Authentication Service (AS) Exchange, Ticket-Granting Service (TGS) Exchange, Client/Server (CS) Exchange. Although both of them are different, in fact,they havesimilar mechanism, function and role.

CAAS solution suggestedby [5], [7] gives a hope for simplicity in implementing the cryptographic technology needs required by various applications run on end-point devices (for example, mobile phones). Although the studies of CAAS are still limited,through this studysome views are gained on how actual business model and CAAS's ways of working are. Some aspectsthat still need to be studied more about the issue of CAAS arerelated to the jurisdiction issues of the cryptographic application on cloud services, the implementation of the Hardware Security Module as a platform for the machine on the cryptography providers as well as the use of Transport Layer Security as a medium of communication between providers andendpoint devices.

This study focuses only on the effort to recognize how the CAAS model proposed by Robinson works through the Kerberos protocol mechanism approach. CAAS itself is a very broad and interesting for further exploration. Especially for CAAS model by Robinson, more further studies may be focused on how to load the performance of endpoint device in running the cryptographic process, crypto key sharing mechanism for a number of applications, as well as the reliability of the CAAS system for using web services.

REFERENCES

[1] H. A. . Ideler, "Cryptography as a Service in a Cloud Computing Environment," Eindhoven University Of Technology, 2012.

[2] S. Hashemi, K. Monfaredi, and M. Masdari, "Using Cloud Computing for E-Government : Challenges and Benefits," *Int. J. Comput. Information, Syst. Control Eng.*, vol. 7, no. 9, pp. 596–603, 2013.

[3] M. Wang and L. Liu, "CRYPTO AS A SERVICE," in *International Workshop on Cloud Computing and Information Security (CCIS)*, 2013.

[4] S. Bleikertz, S. Bugiel, and H. Ideler, "Client-controlled Cryptography-as-a-Service in the Cloud," *Appl. Cryptogr. ...*, 2013.

[5] P. Robinson, "Cryptography As A Service." RSA Europe Conference, 2013.

[6] H. Rahmani, E. Sundararajan, Z. M. Ali, and A. M. Zin, "Encryption as a Service (EaaS) as a Solution for Cryptography in Cloud," *Procedia Technol.*, vol. 11, no. Iceei, pp. 1202–1210, 2013.

[7] P. Robinson, "Applying Cryptography as a Service to Mobile Applications." 2014.

[8] S. Kumari, "Exploring Classical Security Techniques for Cloud Computing Environment," *Int. J. Comput. Appl.*, vol. 4, no. 4, 2014.

[9] S. Fahl and M. Harbach, "Confidentiality as a Service--Usable Security for the Cloud," *Trust. Secur. ...*, 2012.

[10] V. Varadharajan and U. Tupakula, "Security as a Service Model for Cloud Environment," *IEEE Trans. Netw. Serv. Manag.*, vol. 11, no. 1, pp. 60–75, 2014.

[11] H. A. W. Ideler, "Cryptography as a service in a cloud computing environment," Eindhoven University of Technology, 2012.

[12] T. Field, "Cryptography in the Cloud," *Bank Info Security*, 2011. [Online]. Available: http://www.bankinfosecurity.com/cryptography-in-cloud-a-3305/op-1. [Accessed: 06-Sep-2014].

[13] G. Dua, N. Gautam, D. Sharma, and A. Arora, "Replay Attack Prevention In Kerberos Authentication Protocol using Triple Password," *Int. J. Comput. Networks Commun.*, vol. 5, no. 2, pp. 59–70, 2013.

[14] F. Andrianto, "Analisis dan Perbandingan Keamanan Jaringan pada Mekanisme Autentikasi Menggunakan Kerberos dan HTTP over SSL," Telkom Bandung, 2009.

[15] M. K. Consortium, "Why is Kerberos a credible security solution ?," 2008.

[16] K. Wahyu, N. D. Cahyani, and T. Brotoharsono, "Flexible Authentication Secure Tunneling (Fast) Pre-Authentication Protocol Pada Kerberos 5," Bandung, 2009.

