Enhancing Cloud Security Using VKC as a Service

Syed Saqib Raza Rizvi1, Muhammad Asad Ullah2, Sagheer Abbas3, Shahid Naseem4

[1,2]University of Lahore, Lahore, Pakistan
[3]National College of Business Administration & Economics, Lahore, Pakistan
[4]University College of Engineering, Sciences & Technology, Lahore, Pakistan

ABSTRACT
Cloud computing has brought a revolution in IT services infrastructure. Above 20% of worldwide internet based services are already shifted onto cloud computing. With the enormous advantages cloud computing has also barriers to achieve adoptability worldwide. Data security and privacy is the biggest concern of cloud users because of cloud unique environment like ubiquitous computing, remote resources, no control etc. Cryptography is the best known and one of the oldest technique used by man to secure information. AES (Advance Encryption Standard) is considered most secure symmetric key algorithm and adopted worldwide as a new security standard after DES (Data Encryption Standard), but there are some limitations of this algorithm as well. This paper proposes a model which is VKC (Variable Key Block Cipher) extended form of AES, as a service. This proposed model overcome limitations of AES to prevent attacks done in past on AES.

General Terms
Cloud Computing, Security.
Keywords
Cryptography, AES, VKC, Privacy, Threats.

1. INTRODUCTION

There are more than one billion active cloud users, using easy, reliable and cost effective cloud services all around the world in form of social networking, data sharing etc. [1]. Cloud computing offers pool of ubiquitous, on demand and configurable shared computer resources such as storage, networks, applications, and web services over the internet. The biggest motivation behind cloud computing is to shift more of the computational work, tasks and challenges from client side to, unseen and almost unlimited cluster of resources over the internet [3]. Due to advantages of availability, flexibility in obtaining computational resources in a low cost cloud computing gain tremendous adoption in information technology infrastructure worldwide, in the past few years cloud computing has become one of the fastest growing paradigms of modern technology [4]. Cloud computing provides many potential advantages to small and medium enterprises such as low cost scalability, security control, fast deployment, rapid elasticity etc. [5] .In general cloud computing provides three basic types of services i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [2].

With the growing amount of usability and confidential data volume, cloud computing is also facing challenges in the field of privacy and data security [1]. Privacy and security are still biggest barriers against cloud computing large scale adoption [4]. Cloud users have no control and knowledge about the devices which are providing them services because they do not belongs to users [2]. The main security issues of cloud computing are:

1.1 Cloud Security Issues:

1.1.1 Access to Server and Application:

In cloud computing environment administrated access is conducted through internet, which increase the security risk. Data access is most important security policy provided by the user while accessing the data. Every business organization has its own security policy. Security policies must have some considerations about intrusion of data by unauthorized user's access.

1.1.2 Data Transmission:

In most of the cloud environments data is not encrypted during the processing state. Data should be unencrypted before processing, but after the processing state especially for data tramission advance encryption protocols must be used by CSP's to increase availability, confidentiality and audit in resource usage.

1.1.3 Virtual Machine Security:

Multiple instances of same application could execute parallel on one physical machine in cloud computing environment. Multiple instances must be kept isolated from each other to maintain consistent security.

1.1.4 Network Security:

Issues regarding to network security includes DNS attacks, sniffer's attacks etc.

Manuscript received June 5, 2017
Manuscript revised June 20, 2017

1.1.5 Data Privacy:

Data privacy is one of the key security issue for cloud computing, Privacy is concerned with person to person control of information.

1.1.6 Data Integrity:

Integrity in cloud refers to protected from unauthorized deletion, modification, theft of data.

1.1.7 Data Availability:

Availability is major factor which provide access to services, data and tools anywhere, anytime. In cloud computing environment, data is hosted on remote servers accessed by internet if cloud goes off or service became unavailable the data would not be available to user anymore.

1.1.8 Multi-tenancy:

Data of one user should be isolated with other users, as all users are accessing data from the same source.

1.1.9 Data Remainance:

It is the residual representation of data that have been in some way nominally erased or removed.

1.1.10 Confidentiality:

Cloud computing involves a very large number of users accessing cloud services from different access points and applications, each user data has unique importance, so it should be privately managed and secured.

There are number of proposed solutions to overcome the security threats of cloud computing that are:

1.2 Existing Frame Works:

1.2.1 Encryption and Steganography:

Encryption refers to decoding the information using encryption decryption techniques. Stenographic techniques used to conceal one message, file or data into another.

1.2.2 Trusted Third Party:

In this technique there is a trusted third party which provide end-to-end security to data using encryption or stenographic techniques. Both parties rely on the third party providing security. Used in critical transaction communication.

1.2.3 Incremental Cryptography:

This is example of quick transformation of data from. Encryption and decryption applied only on the chunk or a part of data not on to entire data.

Document M (transform) -------→ Document C

M+d = Mx (transform) ----------→ Cx

Cx-d--------------------------------→ Document M

1.2.4 Proxy Re-encryption and identity based encryption:

This is very interesting technique in which every public key contains unique information about user. Third party encryption servers are used for cryptography.

First party (encrypt) ----→ third party (encrypt) ----→ third party (decrypt) ----→ sec party (decrypt)

Third party provide the public key which has information about the first party private key.

1.2.5 Certificate Based Authentication:

In cloud, cloud service provider and mobile user are not from same security domain. Users are identified by their characteristic or attributes therefore attributes of user need to be authorized by trusted unit because traditional identity based access control is not so effective. Certificate is issued to mobile user by certification authority which acts as trust center.

1.2.6 Watermarking techniques:

This technique use adding identified data such as sequence of characters or code to the digital content. This technique is implemented with blend of encryption or stenographic technique.

1.2.7. Security Service Admission Model (SSAM):

Based on Semi-Morkove Decision Model. A complex statistical architecture which compute the probabilities of states and the action performed by the user to attain the state.

In all the proposed solutions and frameworks encryption is the most used and powerful technique. Cryptography algorithms are used to provide security like data integrity, authentication, confidentiality, access control, integrity and availability etc. [7, 8]. Question arises that did user data get actually encrypted, also some of cryptographic algorithms provide insufficient security to user's data especially in cloud computing environment [3].

Overcoming these problems NIST selected AES (Advance Encryption Standard) as information processing standard in 2003 [11]. AES is block cipher, symmetric key algorithm. Number of internal rounds depends upon cipher key length. Key size is variable 128, 192 or 256. AES encryption and decryption involves four steps substitution step, shift row, mix column and add round key [8].

Up till now AES was considered as the most secure encryption algorithm, although many researches had shown that the rigid time space complexity of AES (Advance Encryption Standard) is quit less than DES (Data Encryption Standard) or any other competitor algorithm but still it is matter of concern [12], also many successful cryptanalysis systems are designed to attack AES. The attacks on AES are divided into two categories, attack needs same key and attack does not need same key. The most popular AES attack is known as Cache-time attack in Cache-time attack attacker need same key for cryptanalysis, Dag Arne Osvik et al. demonstrated several Cache-time attacks against AES, and one attack was able to obtain AES keys after only 800 operations in only 65 milliseconds. Warren D. Smith also explained powerful form of linear cryptanalysis which involve affine approximation, appear to break AES-256. Another attack on AES where attacks don't need the same key are implementation attack, a family of differential attacks on the system are proposed which are able to obtain AES keys in 7-round in AES-128, 8-round in AES-192 or AES-256 [11]. Cache time attack could be more realistic, problematic especially when it is executed in cloud computing environment because of several limitations of cloud computing i.e. insecure networks, remote data location, data segregation [2], shared technology, malicious insiders and availability chain [4] etc.

2. RELATED WORK:

Many researches have been conducted around the world to increase security in cloud computing. Fahl et al. proposed a novel approach of confidentiality as a service (CaaS), which included a third party providing and maintaining end to end confidentiality in data, that approach also provided multiple or incremental encryption concept as well [1].

Padhy et al. provided sufficient knowledge about possible security issues and threats faced by cloud computing at that time. They also specified research challenges in the field of cloud computing like service level agreement, cloud data management and security, data encryption etc [2].

Sachdev et al.proposed a new model using AES (Advance Encryption Standard) for enhancement and for better cloud security [3]. Islam et al. also identified some major security threats faced by cloud computing [4]. Nedelcu et al identified some challenges and benefits of cloud computing in banking system [5]. Yadav et al. explained important mobile cloud computing issues, problems and possible existing solutions like encryption, watermarking etc [6]. Bhardwaja et al. did useful comparison of symmetric keys algorithms used to provide security in cloud computing, they also proposed symmetric key algorithms should be considered for the enhancement of cloud security [7].

Mitali et al. provided a detail survey on different cryptography techniques used in modern day crypto systems. They also mentioned some advantages and disadvantages of cryptographic techniques like DES, AES, Blowfish and RSA [8]. Pancholi et al. proposed AES (Advance Encryption Standard) as a secure technique to store data in cloud computing environment [9]. Raghatate et al. also proposed AES as most secure technique for cloud computing confidentiality [10]. Sahmoud et al enhanced AES (Advance Encryption Standard) security by using VKC (Variable Block Key Cipher) [11]. More et al. measured time space complexity of AES algorithm with different variety of inputs.

3. PROPOSED SOLUTION:

To overcome the problem of Cache-time attack and other security issues of AES Shamoud et al. proposed an enhanced version of AES which is VKC (Variable Key Block Cipher) [11]. In this paper we had suggested VKC as a Service (VKCaaS) to overcome most of the cloud security issues created by short comings of AES. The concept of VKCaaS paradigm include VKC as a third party security service provider providing proxy re-encryption security concept and also data will be incrementally encrypted illustrated in Fig.1.

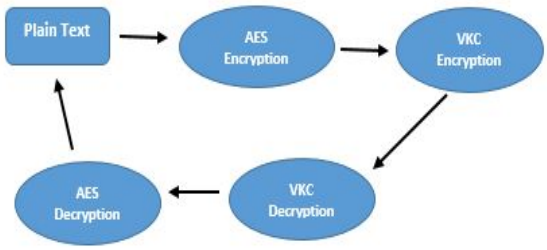

Fig.1 Cryptographic Strategy

3.1 VKCaaS Model:

The detail benefits of VKSaaS is achieved in the following five steps which are:

3.1.1 Step 1 Converting Plain Text Into AES-Cipher:

If Alice want to send data to BOB, in step 1 Alice will encrypt plain text into cipher text with the help of AES algorithm in local machine, and send this AES cipher text to VKC cloud.

3.1.2 Step 2 Converting AES-Cipher into VKC-Cipher:

In the 2nd step VKC cloud will convert this AES cipher text into another cipher text known as VKC cipher. This will implement double encryption on plain text which is AES-Encryption and VKC-Encryption.

3.1.3 Step 3 VKC-Cipher to Service Providing Cloud:

This step will be executed in three sub-steps which are:

3.1.3.1: VKC cloud send back double encrypted data (AES, VKC) to Alice.

3.1.3.2: Alice will send this double encrypted data to service cloud for e.g. Facebook cloud with the help of application provided by the cloud to Alice and Bob to prevail cloud services over the internet.

3.1.3.3: Service cloud send this double incremented data to Bob.

3.1.4 Step 4 VKC Decryption:

Bob will send this double encrypted data to VKC cloud, which will decrypt VKC, VKC cloud will remove VKC layer from the double encrypted data by converting it into only AES cipher (single encrypted), and send data to Bob.

3.1.5 Step 5 AES Decryption:

In the final step Bob will decrypt AES cipher data into plain text with the help symmetric key. Figure 2 illustrate all five steps of VKCaaS.

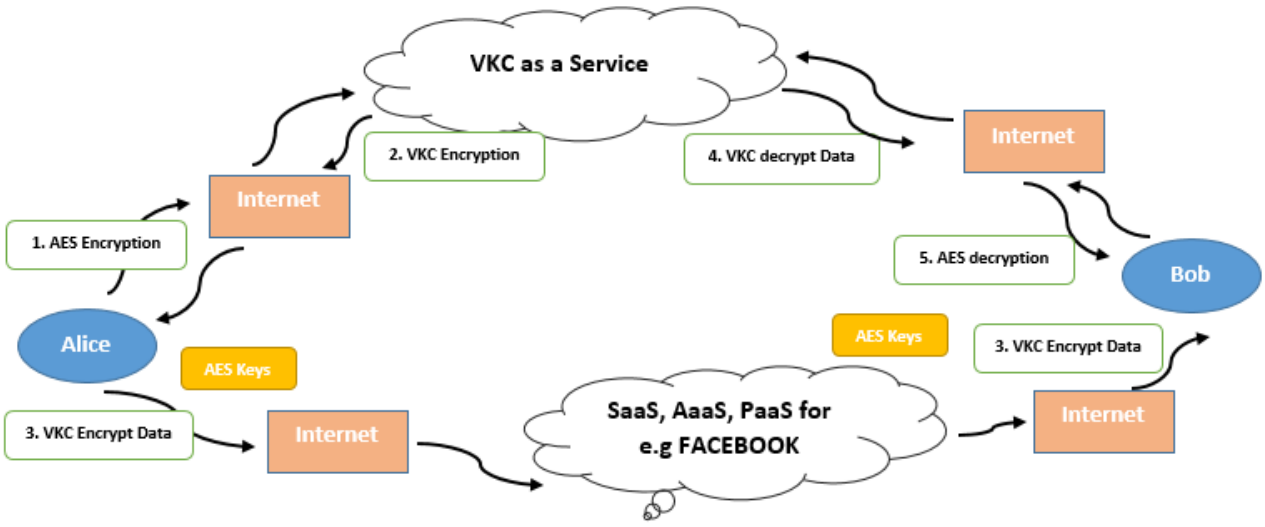

Fig. 2 Communication Model

3.2 Benefits of Proposed Model:

The proposed model will provide following security benefits:

3.2.1 Prevention of Cache Time Attack:

Variable Key Block Cipher make Cache-Time attack almost unrealistic.

3.2.2 Proxy Re-Encryption:

Plain text is secured with the help of double encryption. AES cryptography algorithm will act as First layer and VKC cryptography algorithm will perform as Second layer of cryptography.

3.2.2 Trusted Third Party Security:

VKCaaS cloud act and will provide a trusted third party authentication, which is providing end-to-end security to data.

3.2.4 Use of Static Keys:

As it is clearly defined in the model that AES keys will travel over the internet on more insecure channel, while VKC keys will be static they will only reside in VKC service cloud.

3.3 VKCaaS Data Storage Model:

VKCaaS can also be viewed illustrated in Figure 3, when there is no receiver. Only Alice want to prevail standalone service of a Service Cloud such as data storage.

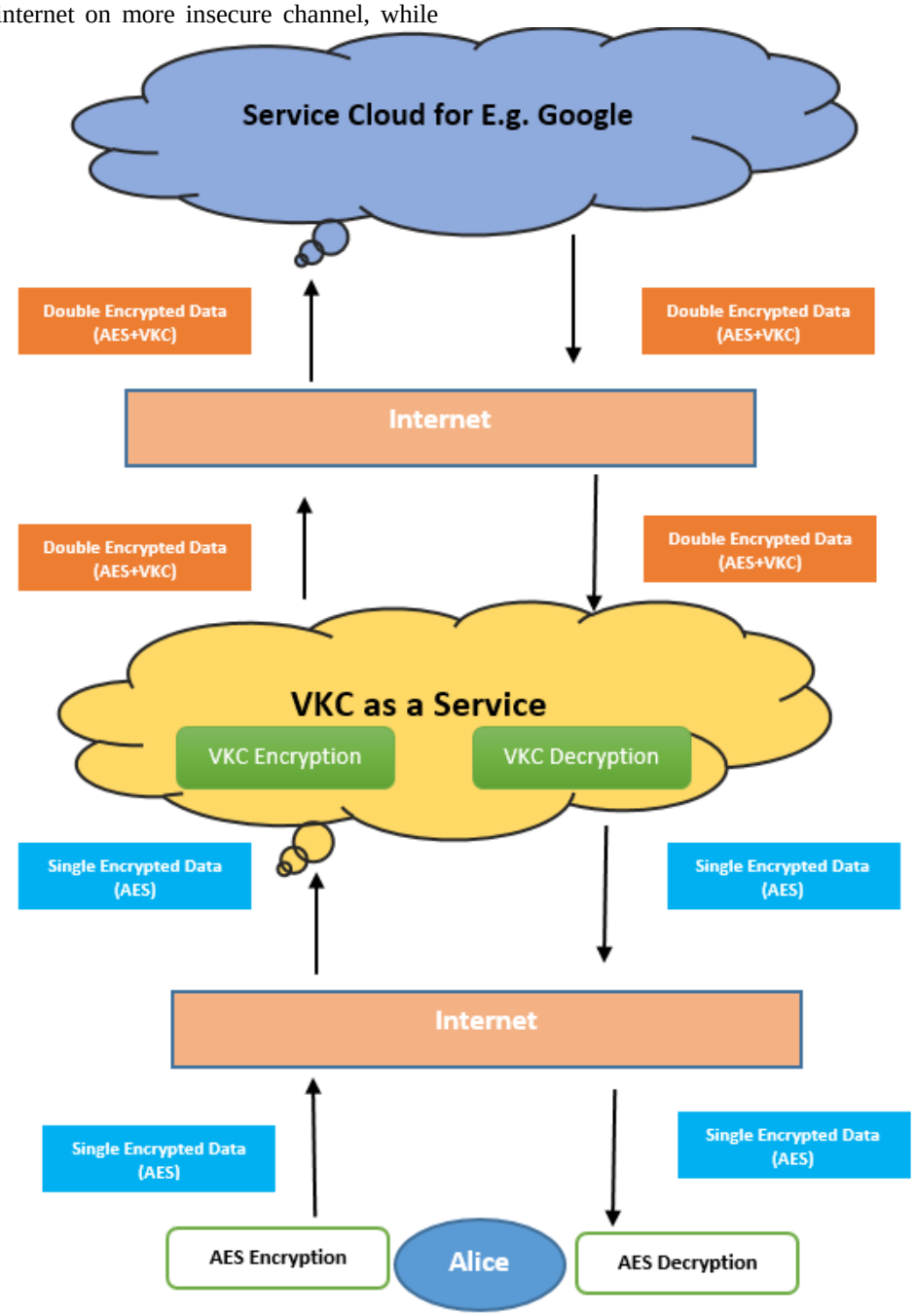

Fig. 3 Data Storage Model

The proposed data storage model deliver security in the following steps that are:

3.3.1 AES Encryption:

Alice will encrypt data using AES in local machine and send this single encrypted data over the internet to VKcaaS cloud.

3.3.2 VKC Encryption:

VKCaaS cloud, will encrypt this single encrypted data again using VKC algorithm, which provides incremental encryption or double encryption to single encrypted data.

3.3.3 VKC Decryption:

While retrieving data, service providing cloud send double encrypted data to VKCaaS cloud which will perform VKC decryption and convert double encrypted data into single encrypted data again.

3.3.4 AES Decryption:

Alice will perform AES decryption on local machine converting, single encrypted data to plain text.

4. CONCLUSION:

AES (Advance Encryption Standard) is still best known cryptographic technique to secure data especially on cloud platform, but there are some limitations of this algorithm are well, like space time complexity, possible liner (Cache Time Attack) and differential attacks. VKC (Variable Key Block Cipher) is a suggested a model VKCaaS as a solution in communication and for standalone cloud services like data storage etc. to prevent cache time attacks, especially in cloud environment.

5. FUTURE WORK:

In future this model can be updated to another upgraded model which can elaborate multiple cloud environment, the model will also suggest how VKC could be effective in inter cloud communication.

Acknowledgements:

We thanks all our teachers, without their help the study was not possible.

References

[1] S.Fahl, M. Harbach, T. Muders and M. Smith, “Confidentiality as a Service—Usable Security for the Cloud”, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 153-162, 2012.

[2] R. Padhy, M. Patra and S. Satapathy, "Cloud Computing: Security Issues and Research Challenges", International Journal of Computer Science and Information Technology & Security, vol. 1, no. 2, pp. 136-146, 2017.

[3] A. Sachdev and M. Bhansali, "Enhancing Cloud Computing Security using AES Algorithm", International Journal of Computer Applications, vol. 67, no. 9, pp. 19-23, 2013.

[4] T. Islam and D. Manivannan, “A Classification and Characterization of Security Threats in Cloud Computing”, International journal of Next Generation Computing, vol. 7,no. 1, pp. 1-20, 2016

[5] B. Nedelcu M.-E. Stefanet I.-F. Tamasescu S.-E. Tintoiu A. Vezeanu "Cloud Computing and its Challenges and Benefits in the Bank System", Database Systems Journal vol. 5 no. 1 pp. 45-58 2015

[6] D.Yadav and K. Doke, “Mobile Cloud Computing Issues and Solution Framework”, International Research Journal of Engineering and Technology, vol.3, no. 11, pp. 1115-1118, 2016

[7] Bhradwaj, A., Subrahmanyan, C.V.B., Avasti, B. and Sastry, H., “Security Algorithms for Cloud Computing”, Procedia Computer Science 85, 535-542, 2016.

[8] Mitali VK, Sharma A. “A survey on various cryptography techniques”, International Journal of Emerging Trends and Technology in Computer Science, vol. 3, no. 4, pp. 307-312, 2014

[9] Vishal R. Pancholi and Bhadresh P. Patel, "Enhancement of Cloud Computing Security with Secure Data Storage using AES," International Journal for Innovative Research in Science and Technology, vol. 2, no. 9, pp. 18-21, 2016.

[10] Vishal R. Pancholi and Bhadresh P. Patel, "Enhancement of Cloud Computing Security with Secure Data Storage using AES," International Journal for Innovative Research in Science and Technology, vol. 2, no. 9, pp. 18-21, 2016

[11] Shabaan Sahmoud, Wisam Elmasry, Shadi Abdulfa, "Enhancement the security of AES against modern attacks by using variable key block cipher", *International Arab Journel of e-technology*, vol. 3, no. 1, January 2013

[12] S. More and R. Bansode, “Implementation of AES with Time Complexity Measurement for Various Input”, Global Journal of Computer Science and Technology. E Network, Web & Security, vol. 15, no. 4, pp.10-20, 2015