ISSN 2587-1943

CRYPTOGRAPHY CHALLENGES OF CLOUD COMPUTING FOR E-GOVERNMENT SERVICES

Hilal Nur Issı 1, Ahmet Efe 2

Original scientific paper

Cloud computing is the popular technology and seems to be very promising for the future trends. In the cloud computing, programs and data are stored and sometimes processed in cloud. So data and programs can easy be accessible anywhere, anytime. Cloud computing is also a very applicable solution for e-government services due to cost effectiveness and efficiency of services. While it eliminates the need of maintaining costly computing facilities by companies and institutes, one of the barriers for cloud adoption is still security concerns. Out of cloud computing is depended upon internet, safety topics such as, confidentiality, authentication, privacy, and data securities are the main concerns. In the cloud, users should search encryption capabilities for preserving and retaining their data. In the same time, they have to protect the functionality of the underlying cloud applications. There are many encryption algorithms to encrypt the data. However, there are new varieties of cyber-attacks developed that threaten the data in the cloud infrastructure. These attacks allow the encrypted data to be re-encrypted, making it incomprehensible by the original owner of the data so that it becomes impossible for the user to decrypt it. This article is written to allow users to understand the working steps and challenges of the algorithms, comparisons of the algorithms and possible solutions for the resent threats in the cloud environment related with cryptography for e-government applications.

Keywords: *Cloud Computing, Cryptography, Data Security, RansomWare, E-government security*

1 Introduction

E-government undoubtedly makes citizens’ lives comfortable and communications easier by its positive effects on increasing efficiency, economy and effectiveness of bureaucracy for the people and providing better communication channels for politicians. Moreover, e-government permits greater access to information, improves public services, and promotes democratic processes. For these reasonable reasons there is a dramatic shift to technology usage and a transition to a “paperless government” which is constantly increasing towards a widespread usage of cloud components and services. The ever increasing usage of electronic technologies and applications in government services has played a significant role in citizen satisfaction and budget minimization. Even though the transition to digital governance has great advantages for the quality of government services it is accompanied with many security threats. One of the major threats and hardest security problems e-government faces are attacks on the cloud environment [30].

Currently, cloud computing is considered to be the newest computing paradigm that offers numerous flexible and consistent services using virtualization technology that is used in the next generation of the data centers. Not only private companies and individuals but also government departments are trying to increase service availability through cloud computing infrastructure. Cloud computing by means of its capacity, resilience and cost minimization that provides the capability to share resources in a pervasive and transparent way, also it has the ability to perform procedures that meet different needs. Moreover, cloud computing offers on-demand services to the users and can have the ability to access common infrastructure.

NIST which is the National Institute of Standards and Technology, identifies five fundamental specifications of cloud computing as on-demand self-service, broad network, access resource pooling, measured service, and rapid elasticity [32]. It also defines that the cloud offers services in four different deployment models (hybrid and community, private, public). It states that cloud providers provide the services in three service models namely infrastructure as a service (IaaS), platforms as a service (PaaS), and Software as a service (SaaS), and it is on the period of development to provide everything as a service (XaaS) [32]. Grobauer at al [33] shows cloud service models together with cloud deployment models, and the fundamental characteristics of this environment.

Due to its capabilities and cost effectiveness, cloud computing has been attracting the attention of many academic entities as well as many organizations [31]. High availability in cloud computing is essential. The availability in the cloud requires the use of cloud resources and services by authoritative users, based on their demands [34]. However, threats related to data confidentiality and service availability can threaten the cloud environment due to its resource multi-tenancy and sharing features [35]. The impacts of the non-availability of services and resources in the cloud are calamitous; and this can lead to a partial or even total failure of delivering the required service [34].

In the cloud computing, programs and data are stored in cloud. So data and programs can easy accessible anywhere, anytime. The explanation of “cloud computing” from the National Institute of Standards and Technology (NIST) is that cloud computing enables 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 [11].

Cloud computing assures that is sharing of computing resources convenient on-demand. Cloud computing directly uses resources, collected of all the computing, via software. Users can buy the computing resource that they are needed.

The deployment model for the discussion throughout this paper would be Public Clouds (and also Hybrid

Clouds). In Public Cloud deployments Cloud platform cannot be relied upon as the cloud infrastructure is run at service provider premises and open for public use. In Hybrid Clouds too part of the cloud infrastructure is run at service provider. Whereas in Private Cloud deployments the platform can be trusted since it is completely within users premises [28].

Cloud computing proposes decreased maintenance and complexity, enhanced scalability, and operational risks. These proposals are realized with the cloud "*Infrastructure-as-a-Service*" (IaaS), "*Platform-as-a-Service*" (PaaS), and "*Software-as-a-Service*" (SaaS). Since the cloud service model is an important architectural factor when discussing key managements aspects in a cloud environment, we are reproducing below the definitions for the service models provided by NIST in SP 800-145, "*The NIST definition of Cloud Computing*":

1. Infrastructure as a Service (IaaS):

The capability provided to the Consumer is to provision processing, storage, networks, and other fundamental computing resources where the Consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The Consumer does not manage or control the underlying cloud infrastructure, but has control over operating systems; storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

2. Platform as a Service (PaaS):

The capability provided to the Consumer is to deploy Consumer created or acquired applications onto the cloud infrastructure that are created using programming languages and tools supported by the Provider. The Consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly the application-hosting environment configurations.

3. Software as a Service (SaaS):

The capability provided to the Consumer is to use the Provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface, such as a web browser (e.g., web-based email). The Consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application-configuration settings.

Cloud computing is a trend in application architecture and development, as well as a new business model. The success of many service providers, with Amazon as a remarkable example, has demonstrated that the model can be applied to a wide variety of solutions, covering the different levels defined in the cloud paradigm. We can consider that cloud computing is at a mature stage, although there remain some limitations and challenges. Cloud computing brings important benefits for organizations that outsource data, applications, and infrastructure, at the cost of delegating data control. The information is processed in computers that the users do not own, operate, or manage. In this scenario, the user does not know how the provider handles the information, and therefore a high level of trust is needed. The lack of control over physical and logical aspects of the system imposes profound changes in security and privacy procedures. Currently there is even a lack of service level agreements between providers and users regarding security [24].

Multiple data centers are run for storing and maintaining the users' data. This multiple data centers are situated in different geographical location in the world. Users' data are stored in the data centers of cloud and controlled and monitored by cloud service providers. Users don't have any control or rights on their data stored in the cloud not even know the location of the data in cloud. This nature of cloud makes many security related issues on the data stored in the cloud. The big problem in cloud is security of data in the cloud. Cloud data are attacked by insiders as well as outsiders in different ways [25].

In the cloud computing, users aren't necessarily able to know where their data is located. They just use whenever they want to. Users upload all their data to the cloud. There is a need to be hidden in this data or to have special data. The user is unaware of where and how the data is stored. In this case, a data security problem arises. Cloud providers are responsible for ensuring the safety of data in the cloud. Cloud providers must provide data confidentiality, integrity, and availability (CIA). Since there is a problem with the data, the institutions that will be held responsible for it are the cloud providers.

Cloud computing which has data in different forms as demonstrated in the figure 1, has some critical problems such as eaves dropping, unauthenticated access, user privacy, various hackers' attacks and leakage and data theft. And this problems are increased day by day.

Data is undefended to attack independently of where it is stored. This is why encryption schemes are used to ensure the security of the cloud-critical data. The user specifies the encryption key. If user wants to change the existing encrypted file again, user will open the encrypted text using this password.

Amongst functional encryption schemes "*Identity based encryption*", "*Attribute based encryption*" and "*Predicate-based encryption*" in all of which, the data owner encrypts the data using public key and also predefines granular access privileges for the rest of the users to access it. Users would then get secret keys from a trusted key server and then decrypt parts of the encrypted data based on their assigned privileges. Such property is very important when different levels of access control needs to be enforced on the encrypted data. But by design they do not provide Output Privacy required in Cloud Computing set up [28]. However, cryptography should ensure:

- *<u>Data Integrity:</u>* information is important when it is true, data integrity supply this vulnerable point.
- *<u>Authentication:</u>* it assigns who you are or what it is.
- *<u>Confidentiality:</u>* it is interested in to prevent cyber theft and privacy.

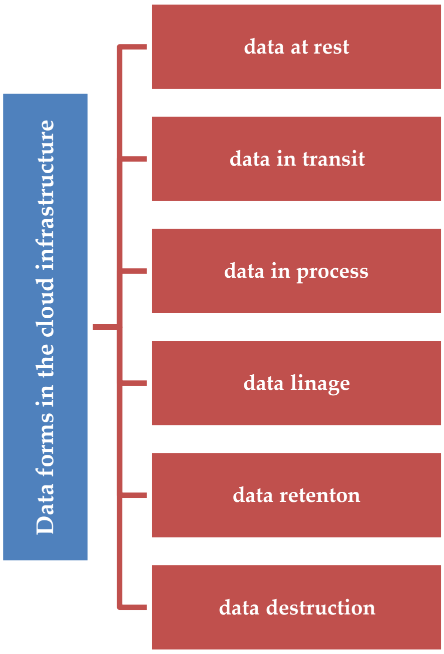

Figure 1 Data Forms in Cloud [25]

2 Cryptography

Cryptography is a science which is used mathematics. ıt uses mathematics in encryption algorithms. Encryption algorithms work two ways. First part is encryption. In this part plaintext is the input and encryption algorithms run on the plaintext. So cipher text is occurs. Second part is decryption. ın this part, cipher text in the input and plaintext is the output. Cryptography terms:

- Sender and Recipients
- Keys: They are important parameters in cryptography. They are used for encryption or decryption
- Plaintext (P) : Unencrypted text
- Cipher text (C) : encrypted text
- Encryption Algorithm (E) : it is used for the transform the plaintext to encrypted text
- Decryption Algorithm (D) : it is used for the transform the cipher text to plaintext with keys
- Cryptanalyze: it means solving cipher text without key.

Plain text → C = D {C, Key}

Cipher text → *C = E {P, Key}* (Fig. 2)

As for as concerns Cloud computing, the security concerns are file systems, network traffic, end user data security and host machine security which cryptography can clear the some extent and thus helps organizations in their unwilling recognition of Cloud Computing. [1]

As is demonstrated in the figure 3, cryptographic methodologies are divided into unkeyed primitives, symmetric key primitives an public key primitives. Security Algorithms are classified broadly as:

- Private Key / Symmetric Algorithms: These algorithms uses the same key to encrypt and decrypt data. Their processing speed is fast. Example: RC6, 3DES, Blowfish, 3DES.
- Public Key / Asymmetric Algorithms: These algorithms use private and public keys to decrypt and encrypt document. If compared to the single key symmetric algorithms, these algorithms have slow speed and thus a high computational cost. Example: Diffie Hellman and RSA.
- Signature Algorithms: these algorithms use keys that are sign and authenticate. Examples: RSA, DH
- Hash Algorithms: In this algorithm, size of data which are used in encryption algorithms, is fixed. Examples: MD5, SHA

a. Symmetric Algorithms

An encryption procedure is symmetric, if the encrypting and decrypting keys are the same or it's easy to derive one from the other. In nonsymmetrical encryption the decrypting key can't be derived from the encrypting key with any small amount of work. In that case the encrypting key can be public while the decrypting key stays classified. This kind of encryption procedure is known as public-key cryptography, correspondingly symmetric encrypting is called secret key cryptography. The problem with symmetric encrypting is the secret key distribution to all parties, as keys must also be updated every now and then [22]. Symmetric algorithms are normally capable of processing major quantity of data and from computing viewpoint. So has lower overhead on the systems and have high accelerate for performing decryption and encryption. Symmetric algorithms encrypt plaintexts as Block ciphers on constant number of 64-bit units or as Stream ciphers bit by bit at a time [10].

Symmetric Algorithms have some problems:

- In symmetric algorithms receiver and sender have to share secret key between each other. In this process third person can learn the secret key.
- Then the third person can decrypt the cipher text and change the context in text. And then, the third person encrypts the new text. So receiver and sender cannot understand the changing.These algorithms have one key. And if hackers have enough cipher text, s/he can learn the key using brute force attack.

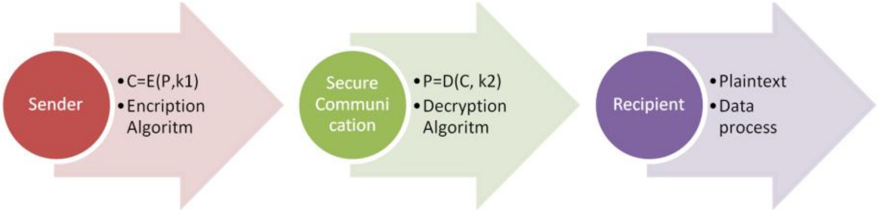

Figure 2 Encryption - Decryption process

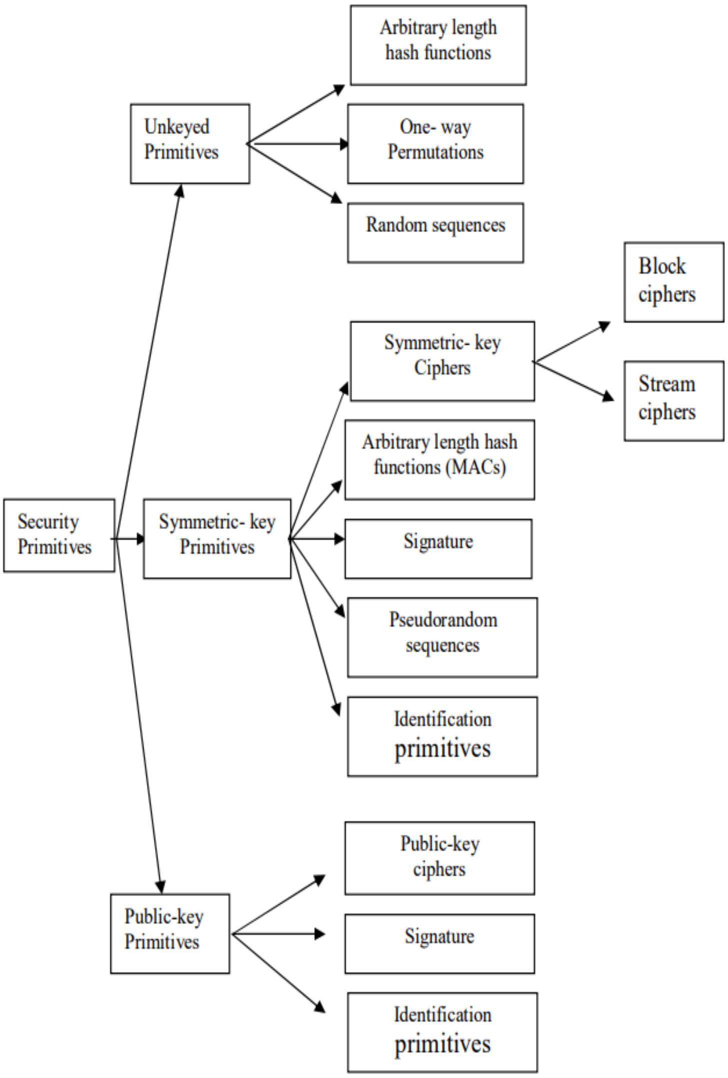

Figure 3 A taxonomy of cryptographic primitives

b. Asymmetric Algorithms

Asymmetric Algorithms use private and public keys to decrypt and encrypt document. The keys are related between each other. Public key shared with everyone. Public key or private key is used for encryption. The other key that isn't use in encryption process is used for decryption. Most popular asymmetric algorithms are RSA, ECC and Diffie-Hellman.

i. RSA

RSA Algorithm named after its inventers (Rivest, Shamir, and Adelman) is best suited for data security Web and Cloud based environments. In the Cloud Computing, the users' data is first encrypted. Then the cipher text stored on the Cloud. In RSA use two keys that are related between each other. Public key is shared with everyone and Private Key is known only to the end user. In this Algorithm, the public and private keys are generating from prime numbers by multiplying that is a mathematical formula, the numbers together.

RSA is being multiplicative homomorphic. It means that multiply the cipher texts to discover the product of the plain text. Therefore the cipher text of the product is the effect of the result. [1]

Digital Signature with RSA encryption algorithm

The digital signature schemes or digital signatures are showing the correctness with a mathematical scheme. RSA algorithm works to encrypting the data while we are transferring it over the network. The idea of using RSA with digital signature is proposed by the authors [4]. Working steps of the proposed scheme:

- Bob wants a document from Alice.
- A record which Bob needs is taking by Alice from cloud.
- The record, using by some Hash function will be divided into small chunks. And finally message digest is occurring.
- Using RSA Algorithm Alice encrypts the message encapsulate with Bob's personal key.
- After that Alice adds her digital signature in the result cipher text.
- For verification of signature, the cipher text will decrypt to the plain text by Bob with Alice public key and Bob's private key.

ii. Diffie-Hellman Key Exchange (D-H):

Diffie-Hellman is a way for swapping keys which are using in cryptography. In the first, to operate for the embed communication determinations a shared hidden key. This key swap operate provides between the two end users that have no previous information of each other to jointly build a published hidden key over untrusted internet. Then a third session key is calculated. So the third key isn't clearly be reproduced by a hacker.

Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm

The authors have selected to make use of a combination of key exchange algorithm and authentication technique blended with an Advanced Encryption Standard (AES) encryption algorithm. This combination is referred to as "Three way mechanism" because it ensures all the three protection scheme of data security, verification, and authentication, at the same time. [11]

When the key in connection is cut, the institution of Diffie Hellman key swap serve it pointless. Until key in connection is pointless without user's special key, imprisoned solely to the lawful user. Developed three way mechanism architecture makes it hard for hackers to fracture the security system, thereby safety data stored in cloud.

- Diffie Hellman algorithm is used to generate keys
- For authentication use digital signature,
- To decrypt or encrypt user's document uses AES algorithm.

All this is implemented to provide trusted computing environment in order to avoid data modification at the server end.

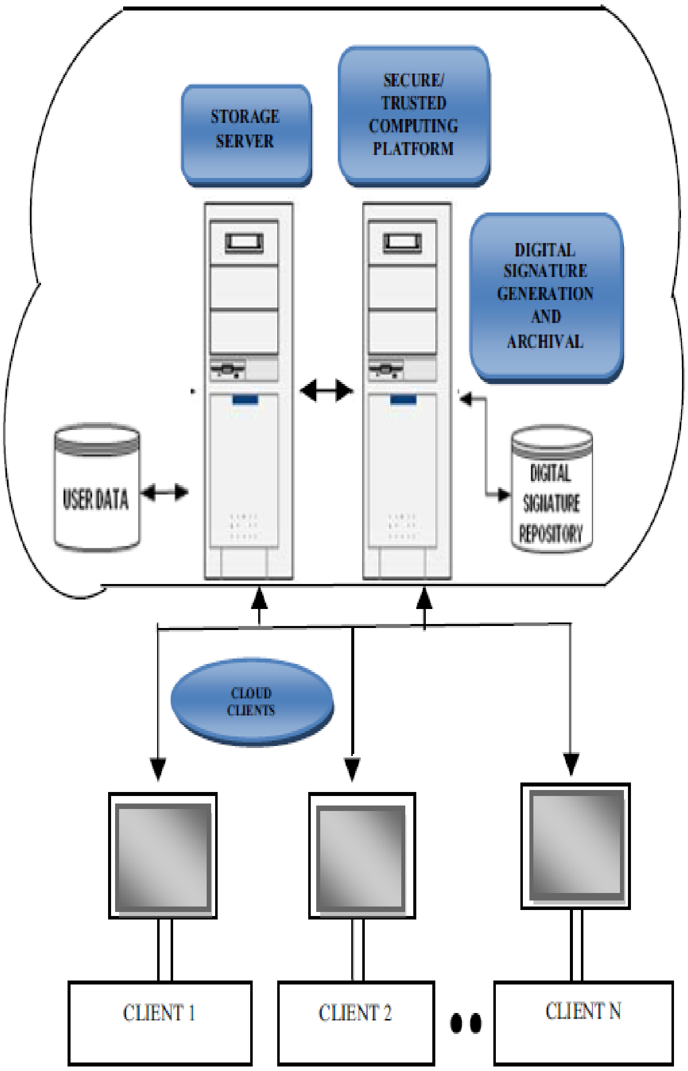
STORAGE SERVER
SECURE/ TRUSTED COMPUTING PLATFORM
DIGITAL SIGNATURE GENERATION AND ARCHIVAL
USER DATA
DIGITAL SIGNATURE REPOSITORY
CLOUD CLIENTS
CLIENT 1
CLIENT 2
CLIENT N

Figure 4 Proposed Architecture

When client is in need the file, client is downloaded from cloud server. File to be downloaded is selected; authentication begins the using digital signature after, to decrypt the saved file uses AES and the file can accessible by the client. [11]

c. Cryptography Summary

✓ When the key size is big, it more difficult to decrypt the encrypted texts, which one by one makes the algorithms effective and efficient.

✓ Using a single secret key algorithm is the most important subjects when working with users who get into touch over untrusted internet. Changing frequently or keeping as secure as possible during the distribution phase in secret key is an only way.

RSA’s strong side, RSA use the two prime numbers, and multiple this numbers for the generate key. When the numbers are reduced the possibility of the decryption by hackers increased.

Prime number growth;

- Bit number required for encryption
- Maybe more powerful machines are necessary.
- Additional memory areas required.

3 Challenges in Cryptographic Operations & Key Management for IaaS

According to NIST for each service model, Figure 5 below uses a building-block approach to depict a graphical representation of the cloud Consumer’s visibility and accessibility to the “Security and Integration” layer that hosts the key management in a cloud environment. As the figure shows, the cloud Consumer has high visibility into the “Security & Integration” layer and has control over the key management in a IaaS model, while the cloud Providers implement only the infrastructure-level security functions (which are always opaque to Consumers). The Consumer has limited visibility and limited key management control in a PaaS model, since the cloud Provider implements the security functions in all lower layers except the “Applications” layer. The cloud Consumer loses the visibility and the control in a SaaS model and, in general, all key management functions are opaque to the cloud Consumer, since the cloud Provider implements all security functions [27].

IaaS cloud service security capabilities (SC), possible architectural solutions (AS) and the cryptographic key management challenges can be demonstrated in the table 1.

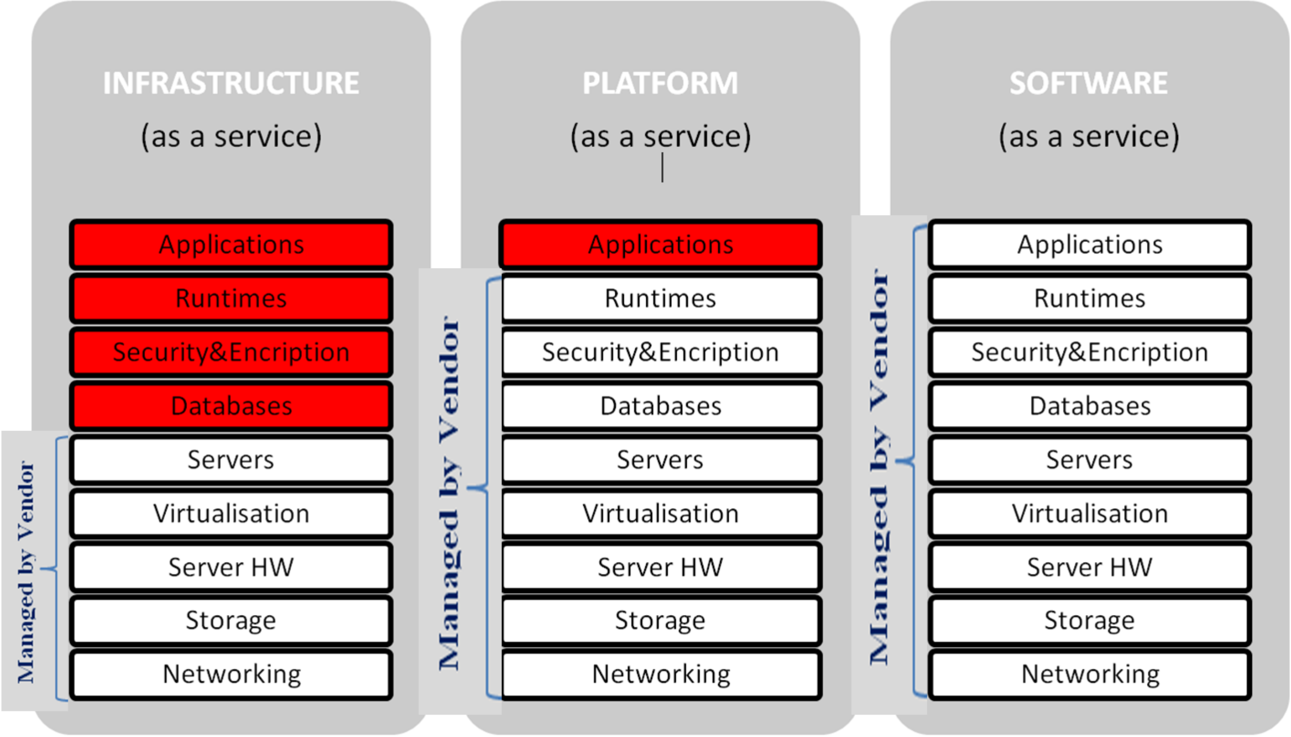

Figure 5 Cloud Service Models and Data Protection (Courtesy of CIO Research Council [CRC])

Table 1. Security capabilities, solutions and challenges in IaaS [27]

Security Capabilities (SC)	Possible Architectural Solutions	Key Management Challenges
IaaS-SC1: The ability to authenticate pre-defined VM Image Templates made available by a cloud Provider for building functional, customized VM instances that meet a cloud Consumer’s needs	the templates can be digitally signed by the cloud Provider.	entails the bootstrapping problem and hence, requires a comprehensive security analysis, rather than just an examination of the key management challenge

IaaS-SC2: The ability to authenticate the API calls sent by the cloud Consumer to the VM Management interface of the cloud Provider's Hypervisor environment	IaaS cloud Provider can implement functionality whereby the VM Management Interface of the Hypervisor only accepts and executes authenticated API calls	Cloud Consumers need to secure the private key of the public/private key pair that is used to sign the VM Management commands on their system
IaaS-SC3: The ability to secure the communication while performing administrative operations on VM instances	SSH can be used to enable the VM instance to authenticate the Consumer using cryptographic means	Cloud Consumers need to secure the private key of the public/private key pair that is used to authenticate themselves, using the best enterprise security mechanisms.
IaaS-SC4: The ability to secure the communication with application instances running on VM instances for application users during cloud-service usage,	The most common technology employed is the Transport Layer Security (TLS) protocol. TLS, just like SSH, can be used to enable the service instance and client to authenticate each other using a cryptographic means.	The secure session requires the presence of an asymmetric key pair (private and public keys) for a service instance and an optional key pair on the client side, as well.
IaaS-SC5: The ability to securely store static application support data securely (data not directly processed by applications)	To support applications running on leased VM instances, IaaS cloud Consumers need secure storage services to store relatively static data such as applications' source code, reference data used by applications, preferred VM Images, and archived data and Logs.	The data that is not processed by or written to by applications can be encrypted at the cloud Consumer site before being uploaded to the cloud Providers file storage service.
IaaS-SC6: The ability to securely store application data in a structured form (e.g., relational form) securely using a Database Management System (DBMS)	The whole database is protected with a single Database Encryption Key (DEK) that is itself protected by more complex means, including the possibility of using a Hardware Security Module (HSM).	Since the IaaS cloud Consumer has administrative control of the subscribed DBMS instance, it has control over the DEK as well.
IaaS-SC7: The ability to securely store application data that is unstructured	This operation requires storage-level encryption similar to Transparent/External encryption	The same key management challenges apply

4 Recent Threats

Cloud use is increasing day by day. The spread of the cloud is actually a good development. However, this development brings new problems as well. Security researchers are found the new vulnerabilities and have released tools that could help users recover files encrypted by two relatively new ransomware threats: PowerWare and Bart.

PowerWare (PoshCoder) aimed the healthcare organizations. ıt was first spotted in March. It noticed because it was implemented in Windows PowerShell, a scripting environment designed for automating system and application administration tasks. New version of PowerWare threat called Locky have recently found by Researchers. Locky uses the extension .locky when cipher text and sends the some ransom note used by the real Locky ransomware. Fortunately, PowerWare is nowhere near as powerful as the ransomware programs it imitates. PowerWare uses the AES-128 encryption algorithm, but with a hard-coded key.

Researchers managed to crack another ransomware program called Bart. Bart first appeared in June. This threat locks files inside password-protected ZIP archives. It doesn't use advanced encryption algorithms. In the Bart infections, affected files original name and extension will changed with .bart.zip. Bart uses ZIP-based encryption. Its key is a complex and very long. Using brute-force methods, the researchers have work out a way to guess the key.

Recent event should be a wake-up call for the ınternet is a dangerous place if your computers and networks are not taking at least basic protection. In 12 may 2017, there was a large-scale massive wave of ransomware attacks in National Health Service (NHS). This malware, known by various names including WannaCry and Wanna Decrypt0r, is understood to have originated from a leak of the US NSA cyber tools. Based on the latest information WannaCry fits well into the classical definition of worm. It has two main parts, a worm module and a ransomware module. All it takes is for one user on a network to be infected to put the whole network at risk. WannaCry's propagation capability is reminiscent of ransomware families like SAMSAM, HDDCryptor, and several variants of Cerber—all of which can infect systems and servers connected to the network. WannaCry ransomware targets and encrypts 176 file types. Some of the file types WannaCry targets are database, multimedia and archive files, as well as Office documents. [18]

There are a few basic measures that must be taken to protect against cyber-attacks. These

- Having an anti-virus software
- Keep this software update
- Prevent direct access to important data
- Back up important files to a local hard drive.
- Keep the data encrypted

There are some products that prevent these attacks. One of them is Malwarebytes software. Software that prevents attacks is wannakiwi software. This utility allows machines infected by the WannaCry ransomware to recover their files. wanakiwi is based on wanadecrypt which makes possible for lucky users to :

- Recover the private user key in memory to save it as 00000000.dky
- Decrypt all of their files

The Primes extraction method is based on Adrien Guinet's wannakey which consist of scanning the WannaCry process memory to recover the prime numbers that were not cleaned during CryptReleaseContext(). WannaKiwi has some limitations;

- Firstly, this method relies on scanning the address space of the process that generated those keys.
- Secondly, we do not know how long the prime numbers will be kept in the address space before being reused by the process.

This is not a perfect tool, but this has been so far the best solution for victims who had no backup. Wannakiwi method has working capacity in 32-bit operating systems. How 64-bit operating systems will work is not yet clearly defined.

A study, proposes a cryptographic scheme for cloud storage, based on an original usage of ID-Based Cryptography (IBC). Proposed solution has several advantages. First, it provides secrecy for encrypted data which are stored in public servers. Second, it offers controlled data access and sharing among users, so that unauthorized users or untrusted servers cannot access or search over data without client’s authorization. During the last decade, IBC has been enhanced by the use of the Elliptic Curve Cryptography (ECC). As a consequence, new ID-based encryption and signature schemes emerged [26].

The greatest feature of the ECC encryption algorithm is that it can provide the security level provided by other public key cryptography systems with lower key values. Along with the development of the technology, newly created encryption algorithms should adapt to this hardware structure. It is very important to secure the newly created wireless networks. With the security provided, it is very important to use the limited bandwidth of the encryption algorithms to be used in wireless networks. ECC is also a very important encryption algorithm for wireless networks with low key usage. As a result, ECC is an open key encryption algorithm with very important advantages that the RSA encryption algorithm can take place [36].

In cloud computing, users have to rely on service providers because they do not have detailed and detailed information about how their data is stored. It is critical to make this a little more secure with hardware-assisted cryptography algorithms built with system-level designs. However, a problem arises when using biometric information for security purposes: To what extent will the security of biometric information be kept confidential? If each biometric data is considered to be a unique key that is unique to the person, it is possible that the person can be used as a security enhancing element in entry and exit. Biometric data are precious biologically derived features that cannot be changed. For this reason, a system design should be made considering the safety of these special data [24].

In the past days, some of the famous people in the cloud, hiding in the clouds of personal data of malicious third parties have taken place in the media claim. This suggests that access to cloud computing should be more controlled. From this, it is reasonable to authorize the use of unchangeable and irrevocable properties of the person during access to the personal account. It is more confidential to check on their own, not directly on the cloud, due to the fact that people have their own specific biometric data, concern for passing third parties, and even distrust of cloud service providers. For this reason, besides personal cipher, besides fingerprint data control and secret key production processes based on received biometric data should be studied included in order to protect accounts from unauthorized access. The secret key is an important parameter to be used in the communication phase with the cloud.

A different approach to other tasks should be designed and tested on an application basis, with an available key from biometric data and the implementation of a hardware module design. As mentioned in [37] and [38], the processing of the fingerprint data with a function similar to the hash function has been used to generate a unique number. The unique ID obtained has been integrated into the designed system and an important step has been taken in terms of its applicability with this aspect.

There are also some specific problems that tries to provide solution for the could privacy. One of them is pCloud. With pCloud’s unique client-side encryption functionality users’ files are safely hidden from any unauthorized access. pCloud Crypto lets users protect their confidential files with high-end security, making it as easy as placing a file in a folder. pCloud's security application encrypts data on user's computer, and uploads only the encrypted version to the servers. Files never leave user's device, so there is no way that anyone receives sensitive information in a plain version. We apply zero-knowledge privacy, meaning that encryption keys are not uploaded or stored on pCloud servers, and we are incapable of viewing user files. The encryption key (Crypto Pass) is only available to the one who creates it, i.e. the user. However this solution is still prone to ransomeware that encript even encripted data making it uneccessible.

Authentication is done by calculating cryptographic hash of the data during encryption and decryption, and comparing the results. There are two popular approaches to that: one is to calculate the checksum of the whole file, another is to calculate checksums of small blocks in the file. The downside of the first approach is that you need to have the whole file in order to authenticate it, which may not be the case. Partial file modifications are also problematic in this case and might also require access to the full file. The second approach is vulnerable to several types of attacks. Most likely, the service provider may construct a version of the file that never really existed by combining different small blocks in different ways. **In** pCloud Crypto we solve this problem by using a tree of hashes (also called Merkle tree, similar to what Bitcoin is using as a central part in its protocol).By now, the combination of all keys and security layers that pCloud uses has proven to be unbreakable.

5 Future Direction

In cloud computing, every day a new weakness can be detected. Developed encryption systems are constantly focused on ensuring that third users do not understand. As we have seen from the most recent attack, making the verb incomprehensible should not be the real transaction. The biggest shortcoming of existing encryption systems is that the encrypted data cannot be secured.

We encrypted a text. The text now becomes one that only the key can understand to read freely. An attacker has received encrypted text that we know is safe for our encryption and encrypted it with an algorithm developed. We have provided the reliability of the data using encryption, but we cannot reach the data at this time. If the assailant tells us that he will give us back the money after we have received his medic, we do not have a thing to do.

The real problem here is the creation of encrypted data in the read-only format. When I say read-only, there is no technology that can change the format in the coded text that I mean. Encrypted text cannot be modified. To be formatted, the encrypted text should be in the format such as jpg, system file, pdf (as visual jpg file), etc.

New attacks, newly discovered weaknesses or new methods put forward are research topics for the future. New research topics determine the direction in which systems go. According to research, the most recent topic in the field of cloud computing cryptography is to prevent re-encryption of cipher text. It is aimed to prevent the attacks that make it impossible to be encrypted by re-encryption.

Furthermore, by the advent of quantum computers, CPU

6 Conclusion

Cloud provides many benefits to its users but it has some security problems due its advanced nature of cloud. Data outsourcing is widely popular due to the computing power of cloud. At the same time, security of outsourced data is a question from all the cloud users [25].

Privacy and security in cloud can be said to be achieved when users have control over information they want to reveal to cloud and who can access their information. Without guarantee of security and privacy users can't make shift to cloud only on the basis of lower cost and faster computing. Certain cloud related standards and cryptographic methods for security are coming to existence, still there is long way to go for public cloud to become a trustworthy computing environment [29].

Cloud computing is arising a popular platform in computing industry. Corporate organizations and private and public enterprise are using the Cloud services. But they are facing with threats which are privacy, data theft issues and security. In the organization is a mandatory requirement that Reducing data storage and processing cost. In decision making process of all the organizations, always the most important tasks is that information and analysis of data. In the cloud, security algorithms are used for needs to be properly used for provide end user security. A lot of techniques about the data protection and to achieve highest level of data security have been proposed by researchers in the cloud. For the acceptable cloud computing is required more works.

Classic Encryption methods make the data incomprehensible, so that they cannot be used even if they are played. Nowadays, the newly developed cyber-attacks are not understood by the original owner of the ciphered encrypted data, and it is impossible to solve the cipher. The most recent example of this type of attack is the WannaCry attack.

According to the latest academic studies; now end users are not using just one encryption algorithm to protect their data. They use multiple encryption algorithms to protect data. Thus, the point where one algorithm is missing is completed with the other algorithm. The latest technological news and technology is to ensure the protection of the encrypted data and to allow the cryptographer to freely use it again when requested.

7 References

[1] Uma Somani, Kanika Lakhani, Manish Mundra, “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing”, 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010)

[2] Gurudatt Kulkarni, Nikita Chavan, Ruchira Chandorkar, Rani Waghmare, Rajnikant Palwe ,“ Cloud Security Challenges” , 2012 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA), 2012

[3] Jeff Sedayao,“Enhancing Cloud Security Using Data Anonymization”, Intel IT - IT Best Practices Cloud Computing and Information Security, June 2012

[4] Mr. Prashant Rewagad, Ms.Yogita Pawar, “Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing” 2013 International Conference on Communication Systems and Network Technologies (2013)

[5] Mark D. Ryan, “Cloud computing security: The scientific challenge, and a survey of solutions” The Journal of Systems and Software (2013)

[6] Duygu Sinan, Seref Sagiroglu, “A Review on Cloud Security”, Proceedings of the 6th International Conference on Security of Information and Networks (November 2013)

[7] L. Xiao-hui, S. Xin-fang, “Analysis on Cloud Computing and its Security”, The 8th International Conference on Computer Science & Education (ICCSE 2013)

[8] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, Guangyu Zhu, “Data Security and Privacy in Cloud Computing”, International Journal of Distributed Sensor Networks (Volume 2014)

[9] Alexandra Boldyreva, Georgia Tech and Paul Grubbs, “Making encryption work in the cloud”, Network Security (2014)

[10] Akashdeep Bhardwaja, GVB Subrahmanyamb, Vinay Avasthic, Hanumat Sastryd, ”Security Algorithms for Cloud Computing”, International Conference on Computational Modeling and Security (CMS 2016)

[11] Mohamed Al Morsy, John Grundy and Ingo Müller, “An Analysis of the Cloud Computing Security Problem”, Proceedings of the APSEC 2010 Cloud Workshop (September, 2016)

[12] Samet Akkuş, “Nesnelerin İnterneti Teknolojisinde Güvenli Veri İletişimi - Programlanabilir Fiziksel Platformlar Arasında WEP Algoritması ile Kriptolu Veri Haberleşmesi Uygulaması” Marmara Fen Bilimleri Dergisi (2016)

[13] Xu An Wanga, Jianfeng Mab, Fatos Xhafa, Mingwu Zhange, Xiaoshuang Luoc, “Cost-effective secure E-health cloud system using identity based cryptographic techniques”, Future Generation Computer Systems -67- (2017)

[14] Chao Yang, Mingyue Zhang, Qi Jiang, Junwei Zhang, Danping Li, Jianfeng Ma, Jian Ren, “Zero knowledge based client side deduplication for encrypted files of secure cloud storage in smart cities, Pervasive and Mobile Computing (2017)

[15] Muhammad Baqer Mollaha,∗, Md. Abul Kalam Azada, Athanasios Vasilakosb, “Security and privacy challenges in mobile cloud computing: Survey and way ahead”, Journal of Network and Computer Applications -84- (2017)

[16] Ping Li, Jin Li, Zhengan Huang, Tong Li, Chong-Zhi Gao, Siu-Ming, Yiu, Kai Chen, “Multi-key privacy-preserving deep learning in cloud computing”, Future Generation Computer Systems (2017)

[17] Leandro Ventura Silva, Rodolfo Marinho, Jose Luis Vivas, Andrey Brito, “Security and privacy preserving data aggregation in cloud computing”, SAC '17 Proceedings of the Symposium on Applied Computing (2017)

[18] Raef Meeuwisse, “WannaCry: Is this a Watershed Cyber Security Moment?”, ISACA Now Blog (May,2017)

[19] Dikaiakos et.al, “Cloud Computing: Distributed Internet Computing for IT and Scientific Research”, IEEE, Volume 13, Issue 5, (Sept.-Oct. 2009)

[20] Liang-Jie Zhang et.al, “CCOA: Cloud Computing Open Architecture”, IEEE (6-10 July 2009)

[21] https://github.com/gentilkiwi/wanakiwi#wanakiwi

[22] Keijo Ruohonen, “Mathematıcal Cryptology” 2014 http://math.tut.fi/~ruohonen/MC.pdf

[23] Santosh Kumar Yadav, “Some Problems in Symmetric and Asymmetric Cryptography” A thesis submitted for the partial fulfillment of the degree of Doctor of Philosophy in Mathematics, 2010

[24] Daniel A. Rodr´ıguez Silva David Gonzalez Martinez, Enrique Argones Rua, “Secure Crypto-Biometric System for Cloud Computing” Conference Paper · September 2011 DOI: 10.1109/IWSSCloud.2011.6049023

[25] S. S. Manikandasaran, “Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage” IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol.6, No1, Jan-Feb 2016 498

[26] Nesrine Kaaniche, Aymen Boudguiga, Maryline Laurent, “ID-Based Cryptography for Secure Cloud Data Storage” http://www-public.tem-tsp.eu/~lauren_m/articles/2013-cloud-IDbased-cloudstorage.pdf

[27] Ramaswamy Chandramouli Michaela Iorga Santosh Chokhani, “Cryptographic Key Management Issues & Challenges in Cloud Services” http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7956.pdf

[28] Sashank Dara, “Cryptography Challenges for Computational Privacy in Public Clouds” https://eprint.iacr.org/2013/272.pdf

[29] Radhika Patwari, Sarita Choudhary, “Security issues and Cryptographic techniques in Cloud Computing” International Journal of Innovative Computer Science & Engineering Volume 2 Issue 4; September-October-2015; Page No.01-06

[30] Aikaterini Mitrokotsa, Christos Douligeris, “E-Government and Denial of Service Attacks” 2008 DOI: 10.4018/978-1-59904-937-3.ch00 https://pdfs.semanticscholar.org/eee6/d5c3e55db3278f9421563e77c3f39ead8441.pdf

[31] Alarifi S, Wolthusen SD. “Mitigation of cloud-internal denial of service attacks”. in Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on. IEEE, 2014.

[32] Mell P, Grance T. “The NIST Definition of Cloud Computing”. National Institute of Standards and Technology (NIST): Gaithersburg, MD, 2011.

[33] Grobauer B, Walloschek T, Stocker E. “Understanding cloud computing vulnerabilities”. Security & privacy, IEEE 2011; 9(2): 50–57.

[34] J. Varia, “Best practices in architecting cloud applications in the AWS cloud”, Cloud Computing. Principles and Paradigms, John Wiley & Sons, Inc. Jan 2011, pp. 459-490.

[35] U. Oktay and O. K. Sahingoz, “Attack Types and Intrusion Detection Systems in Cloud Computing,” vol. 9, pp. 71–76, 2013.

[36] T. Yerlikaya, E. Buluş, D. Arda, „Eliptik Eğri Şifreleme Algoritmasi Kullanan Dijital Imza Uygulamasi“, Researhcgate, 2018, https://goo.gl/mHEE9L

[37] S. Tulyakov, F. Farooq, P. Mansukhani, and V. Govindaraju, “Symmetric Hash Functions for Secure Fingerprint Biometric Systems,” Pattern

Recognit. Lett., vol. 28, no. 16, pp. 2427–2436, 2007.

[38] S. AYGÜN, M. AKÇAY, E. O. GÜNEŞ, „Bulut Sistemleri Için Biyometrik Tabanli Güvenlik Sistemleri“, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:2, No:1, S:15-22, 2016 http://dergipark.gov.tr/download/article-file/401119

Authors' addresses

Hilal Nur Issı 1, MSc Candidate
Yıldırım Beyazıt University
Ankara/Turkey
E-mail: ***hilal.nur.hni@gmail.com***

Ahmet Efe 2,PhD, CISA, CRISC, PMP
İnternal Auditor at Ankara Development Agency
Part Time Lecturer at Yıldırım Beyazıt Universiy
Ankara/Turkey
E-mail: *icsiacag@gmail.com*