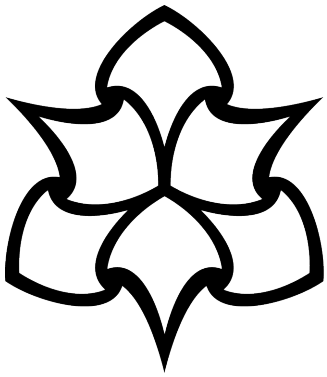

A Survey on Data Confidentiality and Privacy in Cloud Computing

Afnan Aloraini
Manchester Metropolitan University
Manchester, M1 5JD
UK
Afnan-mohammed.o.aloraini@stu.mmu.ac.uk

Mohammad Hammoudeh
Manchester Metropolitan University
Manchester, M1 5JD
UK
m.hammoudeh@mmu.ac.uk

ABSTRACT

Cloud computing is often referred to as the technology of the decade. Current Cloud systems present critical limitations to protecting users' data confidentiality. This survey presents a review of the three essential data security attributes in the context of Cloud computing, namely, availability, integrity and confidentiality. It explores numerous research efforts to enhance the security and privacy of data in the Cloud with a focus on maintaining data confidentiality. Recent solutions are critically analysed, and their advantages and limitations are discussed. The paper finishes with a discussion on the future research opportunities and challenges on data confidentiality in the Cloud.

CCS CONCEPTS

• Security and privacy~Privacy-preserving protocols • Security and privacy~Distributed systems security • Security and privacy~Security protocols • Security and privacy~Virtualization and security

KEYWORDS

Cloud computing, confidentiality, encryption, decryption, cryptography.

ACM Reference format:

A. Aloraini and M. Hammoudeh. 2017. A Survey on Data Confidentiality and Privacy in Cloud Computing. In *Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, United Kingdom, July 2017 (ICFNDS'17)*, 6 pages.
DOI: 10.1145/3102304.3102314

ICFNDS '17, July 19-20, 2017, Cambridge, United Kingdom

ACM ISBN 978-1-4503-4844-7/17/07…$15.00
http://dx.doi.org/10.1145/3102304.3102314

1 INTRODUCTION

In recent years, the world has witnessed a rapid evolution in technology. The boom in wireless and mobile communication technologies has led to a significant increase in the number of Internet users. With the advent of new wireless applications and technologies, the amount of electronic data is growing exponentially day by day. The large volumes of data is one of the key drivers for the demand and the popularity of Cloud computing. Cloud computing is defined by the National Institution of Standards and Technology as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1]. The essential characteristics of Cloud computing are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. The service models for Cloud computing are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Amazon's EC2, Amazon's S3, and IBM's Blue Cloud are examples of IaaS. Yahoo Pig and Google App Engine are examples of PaaS. Google Docs and OneDrive are examples of SaaS.

Cloud computing has been noticed by end users as a low-cost technology trend that offers many efficient on-demand services, such as storage, hardware, and software. However, the availability of these services is dependent on the reliability of an Internet connection. The advantages of Cloud computing are numerous, such as offering more scalable, elastic, and flexible access to virtual computing resources such as processing, storage, and applications. Of all the benefits provided by the Cloud, data storage represents one of the most interesting and attractive prospects, particularly for small organisations due to the low rental cost and the possibility to store and retrieve a volume of data at anytime and anywhere. It is also appealing to large enterprises as it helps to reduce the cost and maintenance overheads of computing services. Cloud computing also attracts individual users, because they can access all data irrespective of the communication medium or access device, such as mobile, laptop, and smart devices. Today, Cloud computing remains a robust technology that offers high data availability. According to Han et al [2] and Wan et al [3], Cloud computing is now

considered to be a utility-along with gas, electricity, water, and phone services.

The security of Cloud systems poses a challenge to both the provider and customers at the same time. Security is a common concern for any technology; however, in the Cloud, security leaks are the main issue that prohibits people from fully adopting Cloud systems. Storing sensitive and private data on Cloud servers is a major concern for clients. Currently, Cloud providers compete to enhance their servers, specifically, in terms of data security and user privacy. However, it is evident that users are increasingly concerned and aware of protecting their data and privacy from attackers. Many incidents affecting users stem from the frequent Cloud failures and successful attacks. For instance, Google Docs was found to be unintentionally sharing users' documents in 2009 [4].

This survey paper outlines the key challenges of data security in Cloud computing and then presents some methods and potential solutions related to enhancing and achieving data confidentiality. The paper is organised into four sections. Following on from the introduction, Section 2 gives an overview of the major challenges facing data security in the Cloud, with a focus on data confidentially. Section 3 presents a survey of recent security solutions to overcome data confidentiality-related security challenges. Finally, Section 4 summarises the main findings of the survey and outlines future research avenues.

2 CHALLENGES OF DATA SECURITY IN THE CLOUD

Security is a critical property of information systems and technologies. Currently, the security of Cloud systems pose a serious concern and risk for organisations who store data in the Cloud. According to Chia [5], trio CIA is the elementary data security concept, which defines the three essential attributes of data security, i.e., confidentiality, integrity, and availability. Data stored in the Cloud can be accessed through various layers. To meet the three above-mentioned security attributes, it is necessary that all the accessible Cloud layers are defended in order to guarantee the security and privacy of data and data owners. According to Yuefa Dai et al. [6], there are three major levels of defence. In the first level, users are verified, authenticated, and issued with digital signatures. The second level provides data protection using encryption. The third level is responsible for the users' data recovery by offering quick decryption services.

The principle of availability is that all data and information is constantly accessible at the level required by the user. Hardening and redundancy are two approaches used to provide the availability of Cloud systems [4]. In terms of hardening, most of the Cloud computing system providers supply platforms and infrastructures placed on virtual machines. For example, Xen is a virtual machine used by Amazon, which is able to provide separate storage and memory virtualization. Virtualization offers the ability to meet service demand from a large number of users, while allowing service providers to secure their system by managing, blocking, and filtering traffic based on IP addresses and ports only. Moreover, large cloud computing system vendors are able to offer geographic redundancy in their Cloud infrastructure. Using different zones, Cloud providers can greatly reduce and protect the system from disruption or failure in a particular location, which can enhance the overall availability of the system (ibid).

Data integrity refers to the data and information storage in the cloud being valid and protected from malicious or accidental modification or changes [7]. Data integrity can aid in detecting data manipulation. In the Cloud, data could be lost or damaged during transmission to or from Cloud data storage. Hence, Cloud service providers should check and maintain the data and computation continuously to prove that the data is intact and in order to detect any potential modification to the data (ibid).

Confidentiality is another essential requirement to ensure the privacy and security of data in the Cloud through applying policies and rules that can limit the access to stored data. To obtain confidentiality in the Cloud, there are two approaches, namely, physical isolation and cryptography. According to Zhou et al. [4], physical isolation cannot be achieved due to the fact that Cloud system offerings, such as data and services, are transferred through public networks. Virtual local area networks and networks' middle boxes, such as firewalls, can be an alternative way to obtain virtual physical isolation. For example, Amazon's vertica deploys the database EC2 and supplies VPN-Cubed and firewall to secure its database. Amazon's vertica database EC2 allows users to access and secure the system through a VPN between the client and vertica, and it provides a firewall to the outside world (ibid). Cryptography provides a more reliable option to ensure data confidentiality. Encryption is the predominantly used method of securing data in storage or during transmission

3 CRITICAL REVIEW OF SOLUTIOS TO DATA CONFIDENTIALITY IN THE CLOUD

In the study of Pant et al. [8], the data security considerations of Cloud computing are discussed, with an emphasis on the security challenges. The authors proposed a solution to achieve data confidentiality and security in Cloud environments using the Rivest-Shamir-Adleman (RSA) algorithm and a steganography technique. The solution consists of three major steps. The first step is to generate an RSA key, which is created by the user. The data is encrypted using the private key, before it is transmitted over the network. The second step employs a steganography technique to hide the cipher text within an image of any extension, such as a GIF, BMP, or JPEG. The data is stored on a Cloud and hidden in these images. The final step, known as the steganalysis process, uses the steganography tool to extract the cipher text from the image. The benefits of this approach are that only authorised users can access the data. The data is protected on the network as it is encrypted. Furthermore, unauthorized users (intruders) cannot easily detect and uncover the encrypted data, even if the intruder obtains the data accidentally, purposely, or captures it. However, this approach

creates a multilevel nature of decryption and encryption, which involves significant computational overhead [1]. Additionally, by increasing the size of the data, the time of computation is also increased. Adding an extra layer of security adds more costs in terms of time and efficiency. Another limitation of this solution is that the image extraction software is required on the machine, where the data is accessed; consequently, the availability of data is bound to the availability of that software on the machine.

Recently, Raju & Sirajudeen [9] presented a solution for data confidentiality to address some challenges of data security. This solution implements the Cramer–Shoup cryptosystem, which is an asymmetric key encryption algorithm, to ensure data security. It comprise three major steps, which are key generation, encryption, and decryption. In the first step, private and public keys are generated. In the second step, data is encrypted and the cipher text is generated, which is then uploaded to the server. The final step includes the decryption of the cipher text, which is done at the receiver's end. The receiver gets the original message if the correct key is provided in the decryption process. The significant advantage of this solution is that data confidentiality is ensured even if the intruder gets access to the data. The risk of unauthorized access to the confidential data and the potential threat of data leakage are eradicated by data encryption. However, the proposed system has been tested with text messages only and does not consider other file formats. On mobile and smart devices, the system running speed could degrade rapidly as decryption occurs at the receiver's end. Moreover, decryption computations could cause battery depletion. Finally, to decrypt the message, a key is provided at the receiver's end, and securing this key is the responsibility of the receiver; thus, the receiver carries the risk of data compromise if the key is lost. Therefore, a new layer or mechanism of security at the receiver's end is required.

More recently, Pitchay et al. [10] presented a solution to ensure that only the owner of files can access them. Although Cloud solution providers guarantee that the inbuilt security solutions deny all unauthorised access, stored files are still accessible to maintenance staff. Numerous clients are reluctant to store data on Cloud servers, knowing that private or confidential data is accessible by various entities, such as the maintenance staff or the file backup process of the Cloud server providers. The aim of this proposed system was to bridge this gap by applying an advanced level of data protection. The author proposed a hybrid solution that combines both RSA and the Advanced Encryption Standard (AES) in its encryption processes. The proposed system uses a removable device to store the private key, which is used to decrypt and encrypt the data. It is mandatory that, at the time of encrypted data upload process, the removable device is plugged into the system. Furthermore, in the case of requesting back the data from the Cloud to the user's computer, the removable device is again required to download the data. The main advantage of this system is that applying a hybrid encryption method leads to a more complicated encryption algorithm, which results in more difficulties for unauthorised users to break the cipher and access the data. The use of the removable device adds a new security dimension to accessing data from the Cloud. In this respect, this system avoids using a single password; it generates random keys and complex combinations, which makes it almost impossible for intruders to decrypt the data. The limitation of the solution is that users need to keep a backup of the removable device with the key. If the removable device is lost, data cannot be downloaded from the server. This adds overhead to this solution; losing the removable device means the data is lost. More overhead is created when the data is to be accessed by multiple users. The USB drives must be password protected so that, in case it is lost, the data is still secure.

Kaur and Wasson [11] presented a Cloud data confidentiality technique based on the Diffie-Hellman algorithm. In addition, their proposed solution utilises the Hash Message Authentication Code (HMAC) to ensure data integrity, and a One-Time Password (OTP) to provide more security. The authors suggested that a Fully Homomorphic Encryption (FHE) technique is more effective than full disk encryption. Nevertheless, there are problems with FHE, including key management, key sharing, access control and data aggregation maintenance, all of which reduce the reliability of the scheme. In this paper, a new model is established for key sharing and management in an FHE scheme. The model is based on the fusion of the Diffie–Hellman algorithm and HMAC. In addition, an OTP is created based on a secret key produced by the Diffie–Hellman algorithm. This algorithm makes a session key between the user and the Cloud, generating a new key between the two every time, before a communication session is started. This algorithm comprises seven steps, beginning with the login and key generation. The third step is the OTP generation, after which the client will enter the operation phase using the HMAC digest, which is the fourth step. After encryption and decryption, users perform data operations. Finally, logout occurs, and the session is closed. Experimental results show that key management time is reduced by establishing a secure channel between the user and the Cloud Service Provider (CSP). This algorithm is reliable and user friendly, as the user does not need to memorise the password to accomplish authentication.

It is evident in the literature that encryption is used in numerous solutions to ensure data security in Cloud systems [12 – 14]. Thus, it is essential to examine the strengths and weaknesses of these algorithms. An abstract model was presented by Kaur & Wasson [11], which uses a hybrid algorithm called Hybrid Encryption RSA (HE-RSA), which utilises asymmetric key cryptographic RSA and symmetric key cryptographic AES. AES is known to perform better than RSA in terms of time complexity, but secure key distribution and management remain a challenge. HE-RSA aims to enhance the security and improve the efficiency of the original RSA algorithm in terms of time consumption, cost and memory size during encryption and decryption processes. In this scheme, a dual encryption process was established to prevent general attacks against the RSA algorithm, including brute-force, timing and mathematical attacks. In HE-RSA, the probability of failure against attacks will be lowered significantly by the selection of exponents larger than 2048 bits. Moreover, HE-RSA dual encryption protects the

transmitted messages against timing attacks and reduces the probability of successful mathematical attacks [15]. This algorithm is efficient in handling various types of attacks, such as brute-force, timing and mathematical attacks. The experimental results presented by the authors show that the original RSA has a much higher execution time than that of the proposed HE-RSA algorithm. Since this work is only an abstract model, its efficiency is still yet to be measured at a larger scale by testing it on large Cloud servers. HE-RSA suffers from high key management overhead, because the number of encryption keys is proportional to the number of users. Therefore, with an increase in the number of users, the number of keys also increase, which is an overhead for the company.

Saroj et al. [16] proposed a scheme to provide strong data confidentiality based on threshold cryptography, while maintaining key management overheads minimal. This scheme consists of three primary objects: the Data Owner (DO), the CSP, and the users. In the beginning, all the users register. The user's credentials are sent to the DO, and then the users are separated into groups by the DO depending on many factors, such as location. Each group has keys for encryption and decryption. Further, the users can authenticate themselves to obtain data from the CSP. The system assumes that the security of the CSP is very high and that the volume of the CSP is very large. The solution utilises a modified Diffie–Hellman algorithm and public key cryptography to maintain secure communication between the CSP and the user. The authors present four algorithms for the proposed scheme. Algorithm 1 is used to ensure that the data communication between the DO and the CSP is secure and that it is used to assure the confidentiality of the DO and the CSP. Algorithm 2 defines the procedure for when a new file is created. Algorithm 3, called the modified Diffie–Hellman algorithm, is used to ensure security in data exchange and communication between the CSP and the user and examines the user's authorisation. Algorithm 4 describes the technique for the threshold cryptography of the user's file. Since data stored in the CSP is encrypted by the DO, only the users and the DO know the encryption key. In addition, the CSP cannot acquire or view client's data. When a user requests data, the CSP sends it to the user in an encrypted form. Hence, the potential for attacks on data during transmission is reduced. However, using many keys affects system performance and requires additional effort to secure them.

A system was presented by Han et al. [2] that combines Attribute-Based Encryption (ABE) and FHE. This scheme allows users to search for encrypted data without a private key. Two different methods based on different requirements were presented for outsourced data computation. The FHE scheme enhances the capabilities of encrypted data, and the Cloud can perform meaningful computing on the data, primarily in the outsourcing of the data and in searching for encrypted data. The main processes of the proposed systems include key generation, encryption, evaluation, searching, and decryption. The major participants of the system are the DO, a large number of users, clusters of Cloud servers, the key generator of FHE and the attribute authority. The proposed solution is efficient and supports searches for encrypted data, even without a private key. Most other existing solutions that provide searching features for encrypted data are based on bilinear maps and do not support multiple keywords, have poor performance, and are less efficient. Yet, they do not provide a mechanism for key management.

3.1 DISCUSSION AND ANALYSIS

In the previous section, we presented a review of some of the prominent approaches to provide data confidentiality in the Cloud. Our study included numerous solutions and techniques based on different algorithms and methods. In this section, all the solutions are further analysed and compared. The strengths and weakness of all the solutions are discussed. The comparative analysis is summarised based on key attributes, such as key management, algorithm efficiency, encryption complexity and the ability to search for encrypted data. All the solutions are listed in Table 1 along with their key attributes. A check mark (✓) shows that a particular attribute is supported and available in the corresponding solution, whilst a negatory mark (×) shows that a particular attribute is missing in the solution. The strengths and weaknesses of each solution are given in Table 1.

Table 1: Comparison of reviewed solutions

Solution	Key Management	Search & Outcome	Improve Efficiency	Strong Enc.
[8]	×	×	×	✓
[9]	×	×	×	✓
[11]	✓	×	✓	✓
[15]	×	×	✓	✓
[10]	✓	×	×	✓
[16]	✓	×	×	✓
[2]	×	✓	✓	✓

The solution provided by Pant et al. [8] is based on cryptographic and steganographic techniques, which makes cryptanalysis more complex. Data is highly protected by this technique, both on the network and on the Cloud. However, by introducing multilevel protection, the robustness of the process is compromised. It is an effective solution for highly confidential documents where the DO or users are limited. One of the core limitations of this solution is that steganography software is required on the user system on which the data is downloaded. Consequently, the availability of data is bound to the availability of the software on the machine. The solution does not discuss the mechanism of the key management, which is another overhead cost.

Raju and Sirajudeen [9] addressed the potential threat of data leakage by implementing the Cramer–Shoup cryptosystem. This is a simple solution compared to the abovementioned approach. The disadvantage of this solution is that key management is the sole responsibility of the user, and there is no way to restore data if the key is lost. This solution does not provide other essential features, such as searching for or outsourcing data.

A hybrid solution was presented by Pitchay et al. [10] based on the RSA and the AES algorithms. In this system, intruders are unable to easily obtain the original data even if they can capture the encrypted messages. A removable device is used for key management. The advantage is that data cannot be decrypted without the device, which holds the private key. Compared to the Cramer–Shoup cryptosystem, this is a comprehensive and more effective solution. The limitation of this solution is that users must plug the USB device in whenever they need to upload or download data. This problem limits the availability of data to the availability of the removable device. Furthermore, no backup mechanisms of the keys or the USB device were defined. Therefore, if the USB is lost, the data cannot be recovered. By implementing a backup mechanism, this solution could be made more effective and useful.

Another hybrid solution was proposed by Bhandari et al. [15]. The authors examined the strengths and security of the RSA and the AES algorithms and proposed an abstract model based on them. A comprehensive examination of the RSA algorithm was conducted, and the efficiency of the algorithm was improved in terms of the running time, cost and memory size. The authors analysed general attacks on RSA and proposed a solution to overcome its vulnerabilities, in order to make the solution more complex and established. Therefore, the major advantage of the algorithm is its improved security and overall efficiency of the Cloud system. The limitation of the solution is, again, key management, which is ignored in many solutions.

Generally, the number of encryption keys is associated with users. A large number of keys introduces new challenges for data security, i.e., key management. For large organisations, solutions that do not address key management become irrelevant, irrespective of their efficiency or ability to secure data. Some approaches have been introduced by researchers to overcome key management challenges, while ensuring data security in Cloud systems. In this regard, a homomorphic scheme was presented by Kaur and Wasson [11]. A new model was established for key sharing and management. The strength of this algorithm is its use of dynamic OTPs to accomplish authentication. The solution is based on the symmetric key algorithm and the Diffie–Hellman algorithm. The session key is exchanged between two parties in the process of communication over a secure channel. The process is efficient and reduces key sharing and management time. However, this model requires enhancements to the Cloud system, as the second party in communication must be the Cloud system. Another limitation of the process is that it does not provide a mechanism for searching for or outsourcing documents.

The solution presented by Saroj et al. [16] also focuses on the issue of key management. The solution utilises a modified Diffie–Hellman algorithm and public key cryptography to maintain secure communication between the CSP and the user. The data is transmitted in an encrypted form, so threats to the CSP are reduced. The authors introduced the concept of a group key, reduced the number of keys and directly related the keys to groups instead of individuals. Therefore, by applying one key corresponding to one group, this solution avoids the key management issue; thus, helping to protect outsource data from attackers. This work is the most comprehensive and established system among the reviewed solutions. The limitation of this system is that the efficiency of the process has not been measured. Furthermore, this solution shares a similar limitation with the solution provided by Kaur and Wasson [11], which is that no search functionality is supported for encrypted data. Both solutions can be improved to facilitate a search functionality, and a complete solution for data security can be presented to appeal to large organisations.

The only reviewed solution that focuses on searching for outsourced data was presented by Han et al. [2]. The solution is based on ABE and FHE. The benefit of the solution is that, along with data security, this scheme allows users to search for encrypted data without a private key. The proposed solution is efficient and supports searches for encrypted data. The limitation of the solution is that it does not provide any mechanism for key management. However, most of the solutions discussed in this paper do not support this functionality.

4 RESEARCH GAPS AND FUGURE RESEARCH AVENUES

Two of the serious limitations of the solutions discussed in the paper are restricting users to a certain machine with special software and the availability of a removable hardware token to access their data on the Cloud. These restrictions are due the inclusion of the new software or configurations on the client side. Such restrictions contradict with the concept of availability and interoperability of Cloud systems, i.e., a user can access the data anywhere from any device. A software prototype is presented by Saleh and Meinel [17], which facilitates secure data storage on the Cloud without interfering with the Cloud operation. The application intercepts communications, encrypts data before transmission to the Cloud and decrypts data when downloaded.

The vast majority of the data confidentiality solutions in the Cloud provide static data storage policies and do not discuss the revocation or modification of these policies. To overcome this problem in the existing systems, when downloading original data, decrypting it, new policies are enforced for encryption before data is uploaded again. However, this is a costly process, especially for the large data sizes. Garrison et al. [18] described this issue, conducted in-depth analyses, and provided the evidence that the cryptographic techniques for securing data by static policies enforcement are likely to bring excessive costs in existing systems. Future work is required to accommodate the above mentioned issues, in order to provide a comprehensive solution without requiring major modifications to existing Cloud facilities.

5 RESEARCH GAPS AND FUTURE RESEARCH AVENUES

With the advent of new wireless and mobile technologies, the recent years have witnessed the evolution of new Internet technologies [19 – 21]. The boom in wireless technologies has

increased the amount of internet users tremendously, thus, the amount of generated and stored data on the internet is growing exponentially. New technologies, including Cloud computing, are evolving rapidly. Cloud computing is appealing to companies, because of its low cost and the lack of overheads, in terms of server maintenance. Cloud computing offers numerous on-demand services, such as storage, hardware, and software, but the availability of these services is dependent on the availability of a reliable high speed internet connection. The security of data in Cloud systems is one of the biggest challenges for Cloud service providers.

This paper illustrated the application of three essential data security attributes in Cloud environments, i.e., availability, integrity and confidentiality. It focused on the confidentiality of the data and explored numerous research papers within the context of Cloud solutions and the enhancement of security and privacy in the Cloud. Particularly, the study focused on security solutions to ensure data confidentiality. These solutions were critically analysed, and their advantages and limitations were discussed and compared. Various solutions provide different models for data security based on cryptography and steganography using different algorithms. However, many security requirements and solutions impose new challenges, e.g., key management. Among the reviewed solutions, two research efforts focus on key management [11 – 16]. These two contributions are mature enough and comprehensive. Furthermore, the solution presented by Han et al. [2] enhanced their features to further consider data searching, outsourcing and security.

6 CONCLUSION

With the advent of new wireless and mobile technologies, the recent years have witnessed the evolution of new Internet technologies [19 – 21]. The boom in wireless technologies has increased the amount of internet users tremendously, thus, the amount of generated and stored data on the internet is growing exponentially. New technologies, including Cloud computing, are evolving rapidly. Cloud computing is appealing to companies, because of its low cost and the lack of overheads, in terms of server maintenance. Cloud computing offers numerous on-demand services, such as storage, hardware, and software, but the availability of these services is dependent on the availability of a reliable high speed internet connection. The security of data in Cloud systems is one of the biggest challenges for Cloud service providers.

This paper illustrated the application of three essential data security attributes in Cloud environments, i.e., availability, integrity and confidentiality. It focused on the confidentiality of the data and explored numerous research papers within the context of Cloud solutions and the enhancement of security and privacy in the Cloud. Particularly, the study focused on security solutions to ensure data confidentiality. These solutions were critically analysed, and their advantages and limitations were discussed and compared. Various solutions provide different models for data security based on cryptography and steganography using different algorithms. However, many security requirements and solutions impose new challenges, e.g., key management. Among the reviewed solutions, two research efforts focus on key management [11 – 16]. These two contributions are mature enough and comprehensive. Furthermore, the solution presented by Han et al. [2] enhanced their features to further consider data searching, outsourcing and security.

REFERENCES

[1] H Elmogazy and O Bamasak. 2013. Towards healthcare data security in cloud computing. In Proceedings of 8th International Conference for Internet Technology and Secured Transactions (ICITST) 9-12 Dec. 2013.

[2] J L. Han. M Yang. C L. Wang. & S S Xu. 2012. Towards healthcare data security in cloud computing. In Proceedings of Second International Conference on (IMAC), 2012, 714-717.Z

[3] Wan. J Liu. and R H. Deng. 2012. HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing. IEEE Transactions on Information Forensics and Security, 7, 743-754.

[4] M Zhou. R Zhang. W Xie. W Qian. and A Zhou. 2010. Security and Privacy in Cloud Computing: A Survey. In Semantics Knowledge and Grid (SKG), In Proceedings of Sixth International Conference on Semantics, Knowledge and Grids 2010, 105-112.

[5] T. Chia. 2012. Confidentiality, Integrity, Availability: The three components of the CIA Triad (2012). Retrieved 06 February 2017 from http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/

[6] B W. Yuefa Dai. Yaqiang Gu. Quan Zhang. and Chaojing Tang. 2009 Data Security Model for Cloud Computing. In Proceedings of International Workshop on Information Security and Application (IWISA 2009), Qingdao, China, 2009, pp. 141-144.

[7] Z Balogh. and M Turcani. 2016. Modeling of data security in cloud computing. In proceedings of Annual IEEE Systems Conference 2016 (SysCon), 1-6.

[8] V K Pant. J Prakash and A Asthana. 2015. Three step data security model for cloud computing based on RSA and steganography. In Green Computing and Internet of Things (ICGCIoT). In Proceedings of International Conference on Green Computing and Internet of Things (ICGCIoT) 2015, 490-494.

[9] S Raju. & Y M. Sirajudeen. 2014. Data security in Cloud Computing using Cramer-Shoup cryptosystem. In Contemporary Computing and Informatics. In Proceedings of International Conference on Contemporary Computing and Informatics (IC3I), 2014, 343-346.

[10] S A Pitchay. W A. A. Alhiagem. F Ridzuan. and M M. Saudi. 2015. A Proposed System Concept on Enhancing the Encryption and Decryption Method for Cloud Computing. In Proceedings of 17th UKSim-AMSS International Conference on Modelling and Simulation 2015 (UKSim), 201-205.

[11] S Kaur. and V Wasson. 2015. Enhancement in Homomorphic Encryption Scheme for Cloud Data Security. In Next Generation Mobile Applications, Services and Technologies. In Proceedings of 9th International Conference on Next Generation Mobile Applications, Services and Technologies 2015, 54-59.

[12] A Carlin. M Hammoudeh. and O Aldabbas. 2015a. Intrusion Detection and Countermeasure of Virtual Cloud Systems-State of the Art and Current Challenges. International Journal of Advanced Computer Science and Applications, 6(6) pp. 1-15.

[13] A Carlin. M Hammoudeh. and O Aldabbas. 2015b. 'Defence for Distributed Denial of Service Attacks in Cloud Computing. Procedia Computer Science, 73 pp. 490-497.

[14] I Ghafir. V Prenosil. and M Hammoudeh. 2016. Botnet Command and Control Traffic Detection Challenges: A Correlation-based Solution. In Proceedings of International Conference on Advances in Computing, Electronics and Communication, 2016. doi:10.15224/978-1-63248-113-9-01. .

[15] A Bhandari. A Gupta. and D Das. 2016. Secure algorithm for cloud computing and its applications. In proceedings of 6th International Conference - Cloud System and Big Data Engineering (Confluence), 2016, 188-192.

[16] S K Saroj. S K. Chauhan. A K. Sharma. and S. Vats. 2015. Threshold Cryptography Based Data Security in Cloud Computing. In Computational Intelligence & Communication Technology (CICT). In Proceedings of IEEE International Conference on Computational Intelligence and Communication Technology, CICT 2015, 202-207.

[17] E Saleh. and C Meinel. 2013. HPISecure: Towards Data Confidentiality in Cloud Applications. 13-16 May 2013.

[18] W C. Garrison. A Shull. S Myers. and A J. Lee. 2016. On the Practicality of Cryptographically Enforcing Dynamic Access Control Policies in the Cloud. In Proceedings of IEEE Symposium on Security and Privacy (SP) 22-26 May 2016,

[19] A Abuarqoub. M Hammoudeh. B Adebisi. S Jabbar. A Bounceur. and H Al-Bashar. 2017. Dynamic clustering and management of mobile wireless sensor networks. Computer Networks, Volume 117, 22 April 2017, Pages 62–75. doi.org/10.1016/j.comnet.2017.02.001

[20] M Hammoudeh. R Newma. C Dennett. S Mount. and O Aldabbas. 2015. Map as a Service: A Framework for Visualising and Maximising Information Return from Multi-ModalWireless Sensor Networks. Sensors, 15(9) pp. 22970-23003. doi:10.3390/s150922970

[21] M Hammoudeh. F Al-Fayez. H Lloyd. R Newman. B Adebisi. A Bounceur. and A Abuarqoub 2017. A Wireless Sensor Network Border Monitoring System: Deployment Issues and Routing Protocols. IEEE Sensors Journal. DOI: 10.1109/JSEN.2017.2672501