JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Techniques for future enhancement for security of cloud computing

Sangeeta Kumari[1]
Mtech Scholar
Computer science and Engineering
SSIET, Dinanagar

Harjinder Kaur[2]
HOD Computer Science and Engineering
SSIET, Dinanager

**Abstract**

In cloud computing data and applications have been maintained using remote servers that is distributed and it utilizes internet. The main advantage of using cloud computing is that it allow user to use applications over the internet and also share files at any computer over the internet. The use of cloud computing has tremendous impact over the IT industry and also it provides efficient use of resources like bandwidth, storage and processing. As the growth of cloud computing increases many users interact with each other and security issues are arising. The cloud computing growth is hampered by these security issues. There are risks of data breach, data loss, unauthorized access, denial of services etc. In this paper the analysis cloud computing security issues and also surveyed various techniques that are used to handle cloud security.

Keywords: cloud computing, security

## 1. Introduction

Cloud computing resource allocation policy varies depending upon SLA(Service Level Agreement). Service level agreement is between client and service provider. Both are bounded by this legal agreement. Violation of this agreement could lead to legal issues. The major flaw in this agreement is boundness of client but freedom of service provider. Cloud computing provides various services but from these services storage is commonly used. The cost of this storage is less hence is used most often. This service is very cost effective so that mass users are becoming the part of it.(Kong, Lei, & Ma, 2018) Intention of mass user is indifferent causing malicious attack on storage resources. Attack model demonstrating transmission between client and server is in figure 1

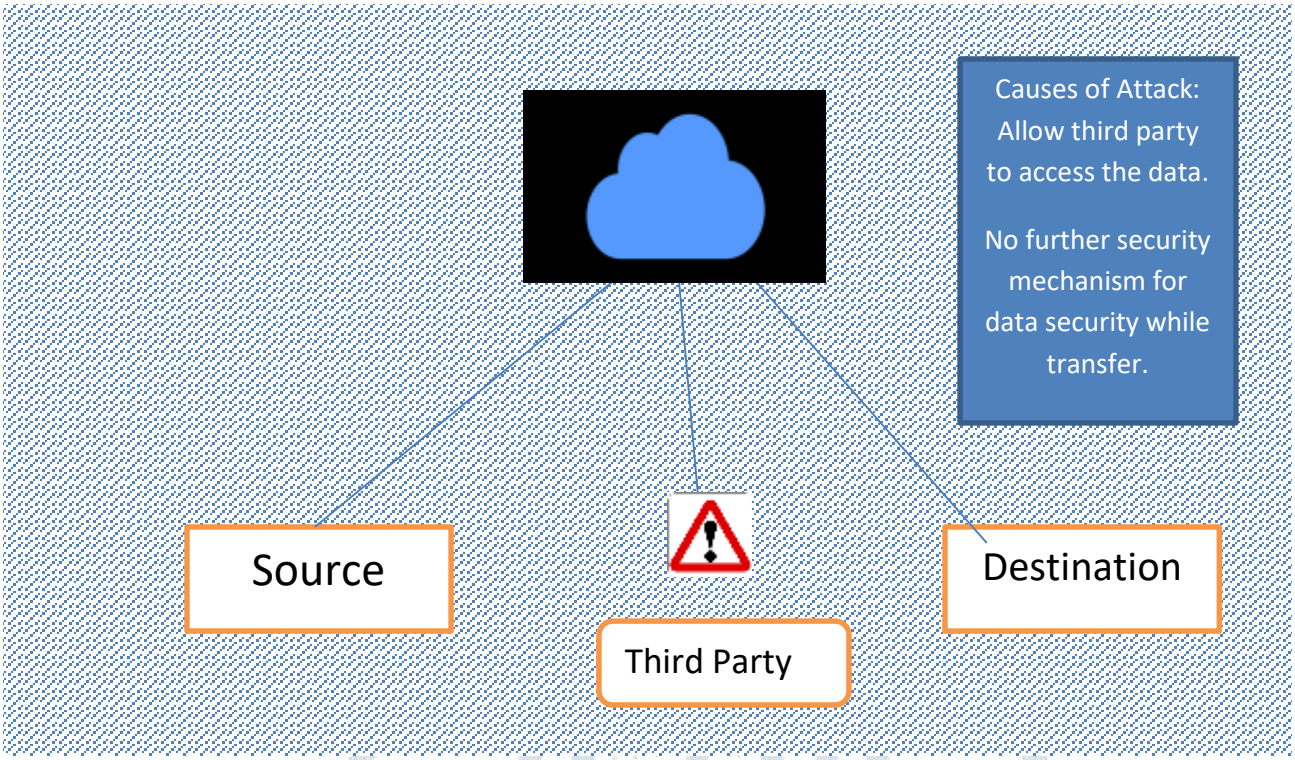


Figure 1: Cloud Attacks

The third party attack is the major issue in the cloud sharing. Clouds are basically created for providing reliable and cost effective service to users. To this end, attack detection and prevention strategies are in place. Attack detection strategies providing reliable cloud service along with after affects are shown in figure 2.

## 2. Attack detection and prevention strategies

Attack causes high energy dissipation and thus additional cost is encountered even though least resources are being used by client causing violation of SLA. Service level agreement affects client rather than service provider. In the era of gathering mass popularity, this could hamper the reliability and utilization of cloud computing. To resolve the issue, attack detection and prevention mechanisms are incorporated within cloud with additional cost from service provider. These mechanisms are listed and discussed in detail as under

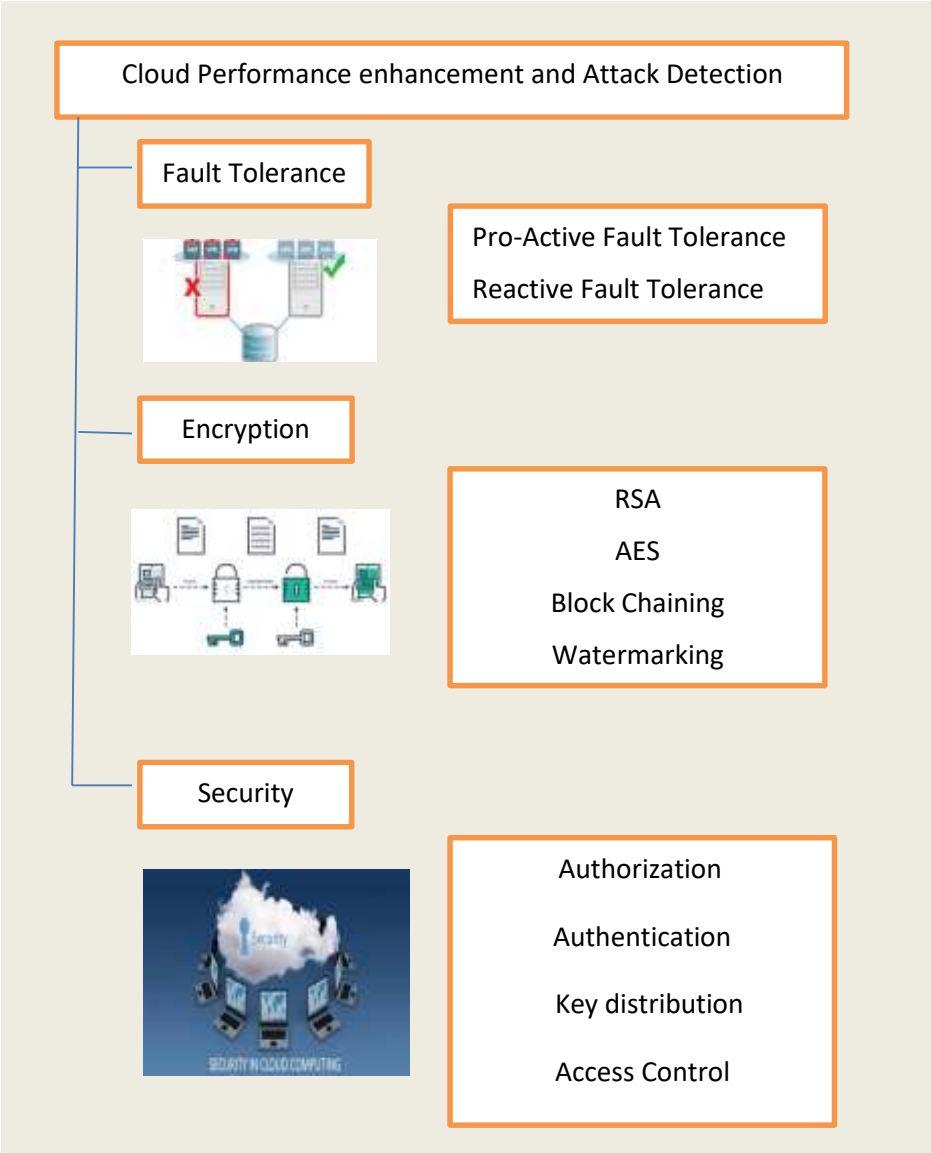


Figure 2: Cloud Security and performance enhancement strategies

### 2.1 Cloud Fault tolerance

Cloud is known for reliability denting the reliability cause mass reduction of people. The reliability degradation is primaily due to attack so a vibal solution to this problem is required. Handling the after effects with the help of fault tolerance effect

#### 2.1.1 Proactive fault tolerance

Proactive fault tolerance is a mechanism in which fault is detected before it occurs. Proactive fault tolerance is an effective mechanism to save energy and prolonged the life of virtual machine. Finding and comparison of distinct mechanisms under proactive fault tolerance is given in table 1.

| Reference | Technique | Advantage | Disadvantage | Finding and future scope |
|---|---|---|---|---|
| (Egwutuoha, Chen, Levy, Selic, & Calvo, 2012) | A Proactive Fault Tolerance | A fault is detected before it impact the system | Energy efficiency is required which is not considered | High performance computing must be merged with migration strategies to improve performance |
| (Egwutuoha, Cheny, Levy, | Energy efficient fault tolerance | Energy is conserved while | Cost is a factor that is increased | Decreasing cost through shadow |

| | | | | |
|---|---|---|---|---|
| Selic, & Calvo, 2013) | | fault handling is enforced | while considering energy efficiency | replication is the need of the hour |
| (Liu & Zhao, 2016) | Fault tolerance as a service at service level of cloud computing | Live migration as a part of fault tolerance causes performance enhancement | Migration time, flow time and overall execution time is high | Migration time can be reduced by considering high performance processor at execution level |
| (Shen et al., 2017) | Based on proposed group sharing data model | Allow multiple user to access and share data in efficient manner | Security is major issue in this section | Security mechanism is not perfect. Try to resolve further |
| (Manzoor, Zhang, & Suri, 2018) | Thread modeling and analysis | Mechanism used to assess potential vulnerabilities that can that can be used to implement cloud goals. | Various attacks encounters in specific clouds | A multi-layer threat analysis model is required to achieve the goal effectively. |

Table 1: Proactive Fault tolerance

### 2.1.2 Reactive fault tolerance

Reactive fault tolerance is a technique is used rectify the faults occurs due to attacks and multi cloud sharing. This techniques are useful in detection and correction mechanism though which recovery can be implemented at an extent. There are comparisons between different reactive fault tolerance techniques in table 2.

| Reference | Technique | Advantage | Disadvantage | Finding and future scope |
|---|---|---|---|---|
| **(Ramamoorthy & Poorvadevi, 2018)** | Smart system and intensive technology | Handle mass information at one data center | Security mechanism is not preventive as hack of people share the data | All private ans public cloud share data and mechanism to handle these type of data effectively |
| **(Gordin, Graur, Potorac, & Balan, 2018)** | Nessus, Metasploit and OpenVAS | Recovery is performed after fault and hence least data loss occurs during tolerance process | Execution time is high as compared to proactive fault tolerance | To reduce the execution time deduplication can be accommodated within the reactive fault tolerance |
| **(Bharadwaj, Bhattacharya, & Chakkaravarthy, 2019)** | Checkpointing | Savepoint is established and hence information I securely recovered | Execution time due to redundant information is high | Execution time can be reduced further by reducing space conservation |
| **(Nie et al., 2018)** | Used appscan techonology | Recovery mechanism can be used to ensure restoration process | Storage conservation is achieved but at the expense execution time | Execution time can be reduced using deduplication mechanism |

| | | | | |
|---|---|---|---|---|
| **(Elhouni, Elfgee, Isak, & Ben Ammer, 2014)** | Cloud security alliance isused | Recovery mechanism ensures that fault tolerance can be achieved through energy efficiency | Execution time is high through this approach | Execution time can be reduced using deduplication mechanisms |
| **(Hahn, Kwon, & Hur, 2018)** | Used message authentication code to check the correctness of partial decryption | Handle decryption in cloud and ensure reliable communication | Execution time is high | Achieve decryption operation but reliability is at stake if size of dataset is high |

**Table 2: Reactive fault tolerance**

### 2.2 Encryption

The guarantee the security of the system encryption considers as one of powerful mechanism. It ensure integrity, confidentiality and certainty to information and protect it from various attacks like forgery , tempering etc. There are various encryption strategies that are used recently. These are as described below:

2.2.1 RSA:

In this encryption strategy public key and private key is consider to find cipher text from plain text using largest two prime numbers. It uses mode n where n is product of two prime numbers p and q and considers as cipher text. The key of RSA algorithm is very difficult to guess so it considered as very secure methodology. In the table below the comparison of various RSA based techniques is given:

| Reference | Technique | Advantage | Disadvantage | Finding and future scope |
|---|---|---|---|---|
| (Shen et al., 2017) | Design base key agreement, Symmetric balanced incomplete block design technique is used | Ability to share group data which improves cooperative environment | The execution time associated with this mechanism is very high | Execution time can be reduced by incorporating folding method by collision detection |
| (Ecosystems, 2010) | In this various variant of RSA is introduced like EAMRSA (Encrypt assistant multi prime RSA | The speed of decryption is highly improved | Numeric values is used that reduced the cipher text conversion speed | The code conversion into universal segment using ASCAI value can be incorporated |
| (Pir, 2016) | Speed monitoring algorithm is used | Safety and speed amplified | Reliability concern is disturbed at each level | Original file can be compared to the transmitted file to determine the difference in formation |
| (Galla, Koganti, & Nuthalapati, 2016) | Security improvement | Implemented theory is improved as security mechanism is necessary | Security improvement algorithm is used and accuracy is ignored at each extent | Accuracy can be increase considering the classifications |

| | | | | |
|---|---|---|---|---|
| (Zhou & Tang, 2011) | Implementation of complete encryption and decryption technique through RSA | Protect data until it decrypted to the other side | Big limitation is that if private key is leaked than it will become useless | Advantageous is many transmission where data is encrypted until it reaches to the destination |

Table 3: RSA Encryption

### 2.2.2 AES:

**AES:** AES is **symmetric** encrypted standard recommend by NIST. AES is used in recent years because of its great competence and easiness. AES is proved to be strong and faster encryption algorithms that use data blocks for encrypt and decrypt the data block. The array of bytes represented data blocks and matrix is used for representing the state of array. The following table describes various AES based encryption strategies:

| Reference | Technique | Advantage | Disadvantage | Finding and future scope |
|---|---|---|---|---|
| (Deshpande, Karande, & Mulani, 2014) | AES-128 bit algorithm designed with symmetric key and Xilinx ISE 14.1 project navigator is used simulation | Network security is achieve at 60 mbps speed of encryption and decryption | Key size is less and can be made more complex for enhancing security | The random key generator can be accommodated for increasing key complexity. |
| (Wei, 2012) | Implemented AES along with FPGA present in this paper and it will security while data transmission | Various FPGA based algorithms are used to increase high speed and less time in key generation | Main concentration on speed and key length only. | The redundancy can be handled using space conservation mechanism |
| (D, 2017) | AES algorithm with hybrid approach with dynamic key generation and dynamic S-box generation is proposed | With hybrid technique complex the data set and make it confusion and defuse it by using strong encryption technology. | Sometime complexity become very difficult to manage | Excellent S-box approach is used to make it difficult for attackers to harm the data while transmission |
| (Soliman, Magdy, Abd, & Ghany, 2016) | Area, throughput and power optimization is covered in this paper | New AES standard is developed to high throughput and low memory consumption | AES-128 bit algorithm is used where multiple key generation steps are use. | Used where power consumption and power saving is main concern |
| (Noorbasha et al., 2019) | AES with X-or operation, Octet substitution with X-Box with Colum, row rotation and mix rotation implementation | It was easy to run and could implement in lowest time on any configuration computer | Key length is less and can easily be decodable. | Manage cryptography and networking simultaneously and main goal is achieved which is information security |

Table 4: AES Encryption

**2.2.3 Block chaining:** A Block chaining is an immutable time stamped series of record of data that is distributed and managed by cluster of computers. It is originally called block chain which means blocks of records which are linked together with the help of cryptography. It is resistant to modification of data. It is an open record maintain book which record the data of two parties who are connected with each other to send and receive data continuously. Comparison of various papers presented on tis is given below in figure:

| Reference | Technique | Advantage | Disadvantage | Finding and future scope |
|---|---|---|---|---|
| (Shen et al., 2017) | Key agreement protocol is used to share data between groups which is secure and efficient in data sharing in cloud computing. | Achieve data sharing among groups on network is achieved in this paper | Extents multiple participants in clouds which caused congestion in transaction and sharing | Future scope is to share data between no of group and maintain security at every level. |
| (Ahram, Sargolzaei, Sargolzaei, Daniels, & Amaba, 2017) | Transaction security mechanism. | Offer secured way to exchange any king of goods, service transaction in efficient manner | During transmission even smallest problem within the block could lead to misleading keys. | Randomization within the key formation mechanism could increase reliability. |
| (Biswas & Technology, 2016) | Integrated technology along with block chaining technology | Purpose a security framework that integrate the block chaining technology for smart cities | The block chaining technique consumes time and no parity bit is establish | The parity bit mechanism can be accommodated to overcome any problem cossesponding to transmission |
| (Halpin & Piekarska, 2017) | Bitcoin technology is used along with cryptocurrency. | Worked with distributed system to achieve high degree of security at each node | Maintaining blocks of every parties and send information to each of them correctly | Used where thousands of people indulge and lakhs of customers are in each block |
| (Shen et al., 2017) | Key agreement protocol, symmetric balanced incomplete block design are used | Support multiple participants in groups and also encourage them to enhance their participation in groups | Security hamper if mass group interact with this system simultaneously | Execution time can be reduced using dedupliction mechanism |
| (Biswas & Technology, 2016) | Block chaining in smart cities | IoT is accommodated along with security mechanism to ensure reliable communication | Energy efficiency is a problem and hence lifetime of network is hampered | Distributed energy efficient clustering algorithm can be used to enhance lifetime of network |

Table 5: Block chaining

### 2.3 Watermarking:

Watermarking is a procedure through which one can cover up helpful data by the utilization of any digital media. Watermarking ensures that the data belongs to the owner and is read by the same user to whom it belongs. Watermarking is an immigrant topic in recent environment for security purpose. The various watermarking based techniques are as given below:

| Reference | Technique | Advantage | Disadvantage | Finding and future scope |
|---|---|---|---|---|
| (Dai, Zhang, & Yang, 1845) | MPEG vedio watermark techonology | A new watermark technology introduced in which copyright is | Degrading the little bit perceptive effect, capability to embed | Watermarking provide best possible security |

| | | | | |
|---|---|---|---|---|
| | | hide through little bit modifications in MPEGE-2 | watermark in short video sequence. | |
| (Cui, Member, Chang, & Member, 2008) | IP water marking using incremental technology at logic synthesis level | The watermarked intellectual property is used | Cost and performance of watermark should be up to date but it I not | Cost factor could hamper security |
| (Matt, 1953) | Electronic watermark technology used | Considerable perception is made in perceptual modeling, security threats and countermeasurs. | Less effective in geometric distortion. | Further progress is needed for handling geometric and temporal distortion |
| (Chang, 2012) | Reversible fragile watermarking technology used | Database watermarking method is used which can effectively authenticate the database integrity and protect the data base | Database size slow down the progress of cloud resources | Watermarking ensures security of highest level |
| (Hsu & Wang, 2012) | Dual watermarking by QR code technique | Solution to the problem of providing gurentee to the copyright images | Not suitable of complex calculations | Watermarking ensure highest form of security |

**Table 6: Watermarking strategies**

### 2.4 Security

Today cloud computing services are utilizes maximum and it becomes backbone of computing zone. Due to usage of cloud computing tremendous amount of information is generated every day and this information is shared among different users so that it will become necessary that security mechanism must be approached. Some security mechanisms are given below:-

#### 2.4.1 Authorization:

The data on the internet is available to all the unauthorized users. Therefore the confidentiality of the data can be lost. So for this purpose authorization is used. The following table describes authorization based techniques:

| Reference | Technique | Advantage | Disadvantage | Finding and future scope |
|---|---|---|---|---|
| (Vishal & Johari, 2018) | Simulation of attacks | Handling data from various types of attacks incurred while transferring the data | Implemented on financial data which can be implemented on limited level | Used in various sector like banking and other financial data. |
| (Koo, Kim, & Lee, 2019) | C41 mechanism used | Efficient mechanism used din defense services | Low bandwidth | Utilize more security mechanism for defense services |

Table 7: Security and Authorization

## 3. Conclusion

In this review paper we have surveyed various security threats and techniques to handle the security in cloud computing. By doing this survey we concluded that the technique which is used for security handling is good and well if it is variable sized as compared to other techniques. This technique improves the performance and storage efficiency of data centers that hold the data and the storage resources can maximize their capacity

to hold the data by removing redundant data. In future more research work can be done on the variable sized security handling techniques that develop an efficient method for high throughput .

## 4. References


Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain Technology Innovations, (2016).

Bharadwaj, D. R., Bhattacharya, A., & Chakkaravarthy, M. (2019). Cloud Threat Defense - A Threat Protection and Security Compliance Solution. *Proceedings - 7th IEEE International Conference on Cloud Computing in Emerging Markets, CCEM 2018*, 95–99. https://doi.org/10.1109/CCEM.2018.00024

Biswas, K., & Technology, A. B. (2016). Securing Smart Cities Using Blockchain Technology. *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 1392–1393. https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198

Chang, J. (2012). Reversible Fragile Database Watermarking Technology using Difference Expansion Based on SVR Prediction. https://doi.org/10.1109/IS3C.2012.179

Cui, A., Member, S., Chang, C. H., & Member, S. (2008). IP Watermarking Using Incremental Technology Mapping at Logic Synthesis Level, *27*(9), 1565–1570.

D, F. J. (2017). Advanced Encryption Standard ( AES ) Security Enhancement using Hybrid Approach, 647–652.

Dai, Y., Zhang, L., & Yang, Y. (1845). A New Method of MPEG Video Watermarking Technology, *1*(4), 1845–1847.

Deshpande, H. S., Karande, K. J., & Mulani, A. (2014). EFFICIENT IMPLEMENTATION OF AES ALGORITHM ON FPGA, 1895–1899.

Ecosystems, D. (2010). Design and Implementation of an Improved RSA Algorithm Yunfei Li, 390–393.

Egwutuoha, I. P., Chen, S., Levy, D., Selic, B., & Calvo, R. (2012). A proactive fault tolerance approach to High Performance Computing (HPC) in the cloud. *Proceedings - 2nd International Conference on Cloud and Green Computing and 2nd International Conference on Social Computing and Its Applications, CGC/SCA 2012*, 268–273. https://doi.org/10.1109/CGC.2012.22

Egwutuoha, I. P., Cheny, S., Levy, D., Selic, B., & Calvo, R. (2013). Energy efficient fault tolerance for high performance computing (HPC) in the cloud. *IEEE International Conference on Cloud Computing, CLOUD*, 762–769. https://doi.org/10.1109/CLOUD.2013.69

Elhouni, A., Elfgee, E., Isak, M. A., & Ben Ammer, K. (2014). Study of security mechanisms implemented in Cloud computing. *2014 World Congress on Computer Applications and Information Systems, WCCAIS 2014*, (2). https://doi.org/10.1109/WCCAIS.2014.6916631

Galla, L. K., Koganti, V. S., & Nuthalapati, N. (2016). Implementation of RSA, 81–87.

Gordin, I., Graur, A., Potorac, A., & Balan, D. (2018). Security assessment of OpenStack cloud using outside and inside software tools. *2018 14th International Conference on Development and Application Systems, DAS 2018 - Proceedings*, 170–174. https://doi.org/10.1109/DAAS.2018.8396091

Hahn, C., Kwon, H., & Hur, J. (2018). Toward Trustworthy Delegation: Verifiable Outsourced Decryption with Tamper-Resistance in Public Cloud Storage. *IEEE International Conference on Cloud Computing, CLOUD*, *2018–July*, 920–923. https://doi.org/10.1109/CLOUD.2018.00136

Halpin, H., & Piekarska, M. (2017). 2017 European Introduction to Security and Privacy on the Blockchain. https://doi.org/10.1109/EuroSPW.2017.43

Hsu, F., & Wang, S. (2012). Dual-watermarking by QR-code Applications in Image Processing, 638–643. https://doi.org/10.1109/UIC-ATC.2012.91

Kong, W., Lei, Y., & Ma, J. (2018). Data security and privacy information challenges in cloud computing. *International Journal of Computational Science and Engineering*, *16*(3), 215–218. https://doi.org/10.1504/IJCSE.2018.091772

Koo, J., Kim, Y. G., & Lee, S. H. (2019). Security Requirements for Cloud-based C4I Security Architecture. *2019 International Conference on Platform Technology and Service, PlatCon 2019 - Proceedings*, 1–4. https://doi.org/10.1109/PlatCon.2019.8668963

Liu, J., & Zhao, J. (2016). Providing Proactive Fault Tolerance as a Service for Cloud Applications, 1–2. https://doi.org/10.1109/SERVICES.2016.26

Manishaben Jaiswal, "DATA MINING TECHNIQUES AND KNOWLEDGE DISCOVERY DATABASE", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.2, Issue 1, Page No pp.248-259, February 2015, Available at : http://www.ijrar.org/IJRAR19D2907.pdf

Manishaben Jaiswal, "ANDROID THE MOBILE OPERATING SYSTEM AND ARCHITECTURE", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.6, Issue 1, pp.514-525, January 2018, Available at: http://www.ijcrt.org/papers/IJCRT1134228.pdf

Manzoor, S., Zhang, H., & Suri, N. (2018). Threat modeling and analysis for the cloud ecosystem. *Proceedings - 2018 IEEE International Conference on Cloud Engineering, IC2E 2018*, 278–281. https://doi.org/10.1109/IC2E.2018.00056

Matt, L. (1953). ELECTRONIC WATERMARKING : THE FIRST 50 YEARS, 225–230.

Nie, W., Xiao, X., Wu, Z., Wu, Y., Shen, F., & Luo, X. (2018). The research of information security for the education cloud platform based on appscan technology. *Proceedings - 5th IEEE International Conference on Cyber Security and Cloud Computing and 4th IEEE International Conference on Edge Computing and Scalable Cloud, CSCloud/EdgeCom 2018*, 185–189. https://doi.org/10.1109/CSCloud/EdgeCom.2018.00040

Noorbasha, F., Divya, Y., Poojitha, M., Navya, K., Bhavishya, A., Rao, K. K., & Kishore, K. H. (2019). FPGA Design and Implementation of Modified AES Based Encryption and Decryption Algorithm, (6), 132–136.

Pir, R. M. (2016). Security improvement and Speed Monitoring of RSA Algorithm, *4*(1), 195–200.

Ramamoorthy, S., & Poorvadevi, R. (2018). Security solution for hybrid cloud information management using fuzzy deductive systems. *Proceedings of the International Conference on Smart Systems and Inventive Technology, ICSSIT 2018*, (Icssit), 457–462. https://doi.org/10.1109/ICSSIT.2018.8748395

Shen, J., Zhou, T., He, D., Zhang, Y., Sun, X., & Xiang, Y. (2017). Block Design-based Key Agreement for Group Data Sharing in Cloud Computing. *IEEE Transactions on Dependable and Secure Computing*, *5971*(c), 1–15. https://doi.org/10.1109/TDSC.2017.2725953

Soliman, S. M., Magdy, B., Abd, M. A., & Ghany, E. (2016). Efficient Implementation of the AES Algorithm for Security Applications, 206–210.

Vishal, V., & Johari, R. (2018). SOAiCE: Simulation of Attacks in Cloud Computing Environment. *Proceedings of the 8th International Conference Confluence 2018 on Cloud Computing, Data Science and Engineering, Confluence 2018*, 152–157. https://doi.org/10.1109/CONFLUENCE.2018.8442733

Wei, W. (2012). An Implementation of AES Algorithm Based on FPGA, (Fskd), 1615–1617.

Zhou, X., & Tang, X. (2011). Research and Implementation of RSA Algorithm for Encryption and Decryption, 1118–1121.