International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 4, May-June 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Survey on Data Encryption and Decryption Models

Saif Ulla Shariff[1], M Ganeshan[2], Mariam Fatima[3]

[1]Master of Computer Science Applications (SCT), [2]Professor,
[1,2,3]Jain Deemed-to-be University, Bengaluru, Karnataka, India

ABSTRACT

Data storage paradigm in cloud computing brings many hard problems on the security. The critical nature of the cloud computing is to incorporate big number of statistics through networks, the need is even more critical. Security should be imposed on information by using encryption techniques to achieve secured statistics storage and access. In this approach some essential protection services along with key technology, encryption and decryption in cloud.

The reason of this paper work is to make a survey of currently current gadgets available inside the market to save encryption keys, how the hacker intrudes into the tool, what are the assaults in the back of robbery of the keys, how are we able to shop encryption keys securely. Under the category of storage devices, USBs (Universal Serial Bus), PDAs (Personal Digital Assistant) and Smart Cards have been tested. Under the class of assaults on devices, attacks from hackers, attacks from malicious code (Trojan Horses, viruses, worms), attacks from PDAs, attacks from Smart Cards, dictionary attacks and brute pressure assaults had been studied. Based on those necessities we've got mentioned and analyzed a proposed machine to store the encryption keys securely to avoid those assaults.

With the speedy development of cloud storage, records safety in garage receives extremely good interest and turns into the top difficulty to unfold improvement of cloud carrier. In this the systematical take a look at of protection researches inside the storage structures. We first present the design criteria which can be used to assess a comfortable garage device and summarize the extensively adopted key technologies. Then, we in addition look at the safety research in cloud storage and finish the new demanding situations inside the cloud environment. Finally, we provide a detailed evaluation among the decided on relaxed storage structures and draw the connection among the important thing technology and the design criteria.

Importance of cloud is due to its unlimited deliver of offerings which includes server, storage of data and what no longer something as a service (Xaas) is viable. As long as customers enjoy its benefits need to take care of the security troubles raisesbecause of its infrastructure that is distributive and as characteristic of the armed provider to the purchaser provider extend their hands to cozy theinformation.This paper specially concentrating in what number of methodprovider will provide protection and how the mechanism works and which is maximum suitable for every and every kind of provider and value involved for the security provision.

Nowadays, the quotes of malicious statistics theft and records destruction are alarming. Governments, organizations and other businesses have lost loads of money and lots of others have closed down because of the sports of dubious hackers and attackers. As records is the existence twine of each organization, there is the need to remotely and securely save the statistics generated day by day through these corporations so as to permit them recover speedy within the event of attach and hack. Cloud storage is wanted here for the far-off information storage. For many institutions, statistics security is certainly one of their essential difficulty whilst sending their documents into the cloud. They fear about their documents being visible or maybe compromised through malicious and dubious people because that's what happened within the past. User debts had been hacked, cloud garage structures failed, files and private statistics have been uncovered. So how are you going to efficiently save you that from happening even if your account gets hacked or something occurs in your cloud garage issuer. Data encryption techniques are required to shield the integrity of the stored facts. In the beyond, many corporations felt comfy allowing the cloud providers to control all their facts, believing that protection risks may be managed thru contracts, controls and audits. Over time it has come to be apparent, but, that cloud companies cannot honor such commitments whilst responding to government requests for records. In this paper, I will attention on cloud storage vendors, cloud protection demanding situations, encryption methodologies.

KEYWORDS: *Cloud Computing, Authentication, Encryption Algorithm, Security, Privacy, Cloud storage system, issues in cloud storage, data protection strategies*

How to cite this paper: Saif Ulla Shariff | M Ganeshan | Mariam Fatima "A Survey on Data Encryption and Decryption Models" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-4, June 2021, pp.593-597, URL: www.ijtsrd.com/papers/ijtsrd42364.pdf

IJTSRD42364

1. INTRODUCTION

Cloud computing is to boom capacity. Cloud computing is a carrier-oriented architecture. Cloud computing is an on-demand statistics technology products and services. Data garage paradigm in cloud computing brings many tough problems on the security and overall performance of the gadget. Securing information is continually of plays an importancerole. Data safety is a critical component of the first-rate of a carrier in cloud.

In this proposed gadget public key encryption set of rules, before storing the touchy information in cloud. When the authorized user requests the records for utilization then information is decrypted and then supplied to the end person. The particular motive of finding a way to store encryption keys in a manner. Encryption keys are used to defend valuable records. If the secrecy, integrity or availability of the keys are broken, then the secrecy, integrity or availability of the valuable facts may be damaged. In this paper we are going to check out exceptional garage gadgets. We can even speak how a device may be built as a way to shop encryption keys securely.

The improved length of records not best causes luxurious storage overhead, however additionally introduces complex information control, incurring extraordinary burden to the customers. Based on the concerns above, increasingly users choose emigrate their data to the far-flung garage servers, that allows you to keep away from the power buy and the difficult information management. However, because the records are out of person's bodily control, a set of security challenges arises, arousing the customers' worries approximately whether their information are safe for the following reasons. First, the consumer's privateness is under the hazard of malicious adversary, because the touchy data (e.g., Non-public e-mail, financial records, health recode) may be found out or altered without the facts proprietor's permission. Second, the person's information can be on the danger of being unavailable due to the sudden accidents or unsuitable operations, that allows you to critically affect the user's business (e.g., The web records operations). Thus, statistics security towards unprivileged access and facts availability are the two problems.

Cloud computing has emerged as an impotent commercial enterprise version where computational sources are rented to customer by means of company. Virtualization era is fundamental for cloud computing. The offerings provided by the service provider may be categorized into three kinds which are infrastructure as a provider (Iaas), software program as a service (Saas), platform as a service (Paas). In general cloud era is defined in three types inclusive of public cloud wherein services are furnished to every person. Private cloud wherein offerings are provided to particular personal organization which owns the privilege of cloud services and the remaining is network cloud wherein one-of-a-kind companies' percentage the assets between the min orders to resolve they're not unusual troubles. In cloud era there's a need of sturdy protection version due to the fact the programs and records of different tenants will use same resources which may be prone to safety assaults. Vulnerability in working gadget or application may be exploited by way of attacker to generate attacks which may goal physical infrastructure or virtual machines of different users. The vital thing in attaining protection is using cryptographic strategies. In standard keys are used in encryption and decryption techniques.

The off-website online, confirmed production structures are managed with the aid of skilled and experienced admins that few businesses should in any other case come up with the money for themselves. Cloud Storage has also been growing in recognition lately because of a few of the equal motives as Cloud Computing. Cloud Storage promises virtualized garage on call for, over a network based on a request for a given great of service (QoS). There is no need to buy garage or in a few instances even provision it before storing data. Your simplest pay for the quantity of storage your records is definitely ingesting. Cloud garage is used in many distinctive approaches. For instance: nearby facts (consisting of on a pc) may be subsidized as much as cloud storage; a virtual disk can be ―synched‖ to the cloud and allotted to other computers; and the cloud can be used as an archive to retain (below coverage) information for regulatory or other functions. For applications that offer statistics immediately to their clients through the community, cloud storage may be used to save that information and the customer can be redirected to a region at the cloud garage issuer for the statistics. Media such as audio and video documents are an example of this, and the community necessities for streaming data documents may be made to scale with a view to meet the call for without affecting the software. The kind of interface used for this is simply HTTP. Fetching the document may be achieved from a browser while not having to do any unique coding, and the right application is invoked automatically. But how do you get the file there inside the first region and the way do you ensure the storage you use is of the right type and QoS? Again, many offerings divulge an interface for these operations, and it's now not surprising that a lot of those interfaces use REST principals as nicely. This is typically a records object interface with operations for developing, analysing, updating and deleting the man or woman statistics gadgets thru HTTP operations

2. METHODOLOGIES

1. Public Key Cryptosystem

In order to triumph over the demanding situations within the present cloud is safety and less garage space. We have proposed new system for supplying protection and much less garage area in cloud. In our paintings we imparting security by the use of the public key algorithm RSA (Ron Rivest, Adi Shamir, Len Adleman). The RSA Algorithm offers the excessive securityin excessive capacity information encryption technique's is a public key cryptosystem that uses keys specifically publickey and private key for Encryption and Decryption respectively. This ensures the excessive diploma of safety. Especially private key guarantees the confidentiality, such that no other person (unauthorized) can view the uploaded document except the statistics owner. Below Diagram shows, First the user has to first input into the web page and request for registration. The user has to fill all of the details after which submit the shape then it will deliver the message registered successfully. If the person was already registered, he can at once log in into the machine and upload the document. User want to upload the document he/she browses the record and click on the upload button then it'll show the message like report uploaded efficiently and the cloud will generate the keys: public key & non-public key. The public key is published however the non-public key is despatched to the user electronic mail which changed into given at the time of registration. That way the data is encrypted and the keys are generated. As soon as the user requests for the view documents the cloud provider will ask for the non-public key. If the accurate personal key's given by using the user, the cloud provider will decrypt the textual content record and displays it to the user. If the personal key is inaccurate then it shows the encrypted facts layout handiest now not the authentic file.

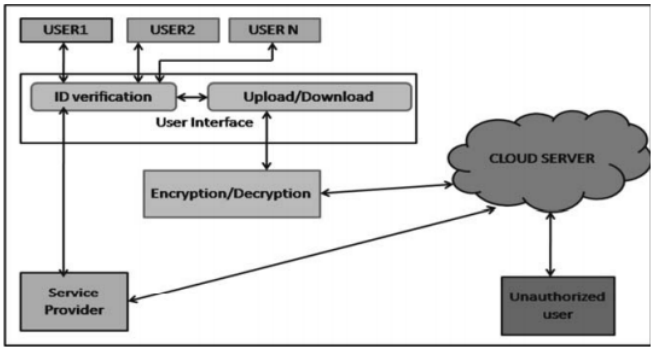

Fig 1(public key system)

2. Storing encryption keys

When an external device is hooked up to the pc there may be usually a chance for unlawful or unauthorized get entry to private records and mystery keys which are stored in the external storage. The hacker generates a bug over the Internet which can replica or block the keys form the outside tool or hard disk. For example, consider an electronic mail virus program which offers the manage access to the hacker who has generated that virus. Similarly, if the same virus software can be extended to get right of entry to the facts from the outside garage and give the total control to the hacker, then the hacker can both copy the important thing or use the important thing.

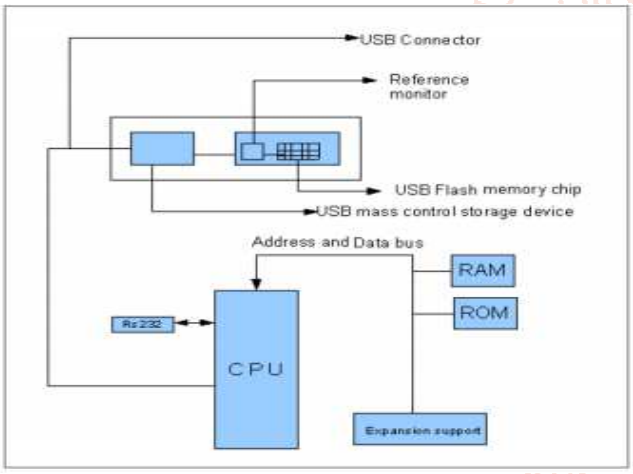

Fig 2(Encryption key storage)

3. Key management for secure cloud

Managing the keys is a maximum important component inside the cloud surroundings which will provide synchronisation for information float within the networks. Encryption is the primary aspect to assure the security but with lot of computational energy and the keys generated through encryption may be a hassle in terms of storing the ones keys which couldn't be in the cloud due to its dynamic nature so it needs the key to be with the client to avoid overweening computations for the decryptions inside the database for the records retrieval.

The following are the prevalent prerequisites for the important thing management:

a) The companies which might be acting the important thing control want to be authenticated and to verify them empowerment to perform these capabilities.

b) The affiliated commands and their records need to be resistible to the spoofing.

c) Capable of determining the undiscovered and unauthorised alterations to find out the integrity

d) Secret and personal keys are auspices from the wildcat revelation.

e) Keys and the facts about their logs are also protected from the spoofing.

f) The security strength of the safety mechanism used for the key management

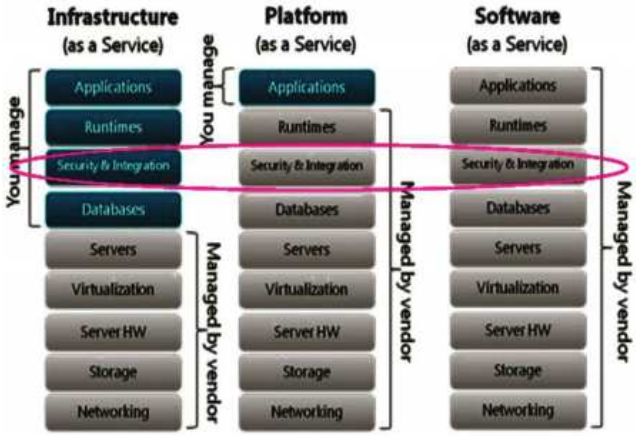

Fig 3(Cloud services comparison)

A] Iaas: In this carrier where the security and integration are taken care by using the consumer and as it is very flexible in order that purchaser positions the assets in the shape of VM's or there's a threat of using leased VM's which permits the checking via default and the assured Vm's have to be attested to ensure the assured get entry toit. As soon as Vm is parameterised and it is released on provider platform to provider the customer via becoming the jogging example. To create a going for walks VM instance it ought to continue after the VM creation. There are exceptional predefined stages for the security in Iaas.

Solution: The essential worry of the clients even as taking the predefined VM photographs from the provider both its miles veritable or no longer so that you can clear up this fear the templates have to be digitally ratified so that it wishes public and private keys to do so and again it's miles company duty to store them securely at the same time as in use additionally which is by means of the use of the FIPS a hundred and forty-2 confirmed module for cryptography by means of NIST and it makes provider answerable for the offering of public key in an attested way

B] Paas: The purpose of a Platform as a Service (Paas) imparting is to give a computational level and the fundamental set of use advancement gadgets to Consumers for growing or sending applications. Despite the reality that the hidden OS level on which the improvement apparatuses are facilitated is understood to the Consumer, the Consumer does now not have control over its layout capacities and therefore the ensuing operating surroundings. Shoppers communicate with these gadgets (and related statistics, for instance, development libraries) to create custom applications. Purchasers would possibly likewise require a stockpiling base to save both helping information and application records for testing the software usefulness.

C] Saas: Saas services give get right of entry to packages facilitated by way of the cloud Provider. A Saas cloud Consumer would possibly need to collaborate with these utility cases safely (through putting in place relaxed sessions and solid validation) and hobby the special software peculiarities, contingent on the set of relegated authorizations or by means of watching for their holed-out

parts (which provide the concurs). Moreover, some Saas Consumers may likewise want to shop the statistics produced/treated through the ones applications in a scrambled shape for the accompanying motives: (a) to counteract presentation in their company statistics, because of loss of the media used by cloud Providers; (b) surreptitious assessment in their records by using a Saas co-occupant or by way of a cloud Provider govt. In spite of the truth that the preceding peculiarity (comfortable reference to application) is given by way of the Saas Providers, the second gimmick (putting away statistics in an encoded shape) proper now need to accept altogether by way of the Saas Consumer.

Solution: There are two operational situations right here. On the off hazard that everyone fields within the database want to be encoded, then the encryption skills want to live with the cloud Provider because of the sheer scale of. Then once more, if everyone cloud Consumer wishes specific encryption of a subset of fields, and considering the fact that this subset adjustments with every patron; all encryption operations need to happen on the consumer (cloud Consumer). The key management challenges for every of the 2 options are examined underneath after a concise portrayal of the associated design arrangement.

4. Techniques in cloud storage

A. Block Cipher:

In this technique ciphering, information is encrypted and decrypted if statistics is in from of blocks. In its simplest mode, you divide the obvious textual content into blocks which are then fed into the cipher machine to produce blocks of cipher text. ECB (Electronic Codebook Mode) is the basic shape of block cipher where records blocks are encrypted without delay to generate its correspondent ciphered blocks. More dialogue approximately modes of operations can be mentioned later.

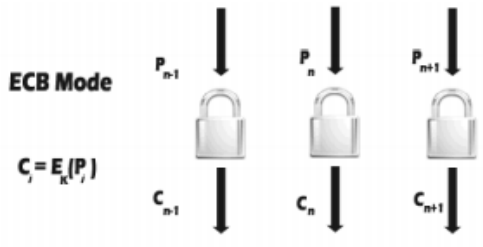

Fig 4(Block cipher)

B. Stream Ciphers:

Stream cipher functions on a move of data with the aid of running on it little by little. Stream cipher consists of two essential additives: a key circulate generator, and a blending function. Mixing feature is normally just an XOR feature, whilst key flow generator is the principal unit in movement cipher encryption method. For example, if the key flow generator produces a series of zeros, the outputted ciphered stream will be identical to the authentic simple text. Shows the operation of the simple mode in circulate cipher.

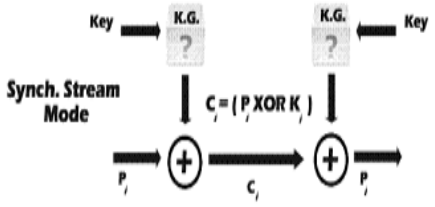

Fig 5(Stream cipher)

I] Symmetric Encryption:

In this sort of encryption, the sender and the receiver agree on a secret (shared) key. Then they use this secret key to encrypt and decrypt their sent messages. A and B first agree at the encryption method to be used in encryption and decryption of communicated statistics. Then they agree on the name of the game key that both of them will use on this connection. After the encryption setup finishes, node A begins sending its facts encrypted with the shared key, on the other facet node B makes use of the same key to decrypt the encrypted messages.

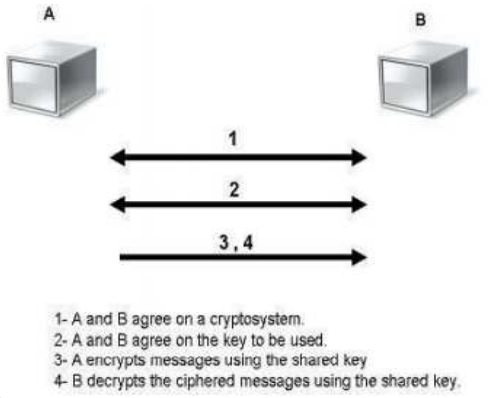

Fig 6(Symmetric encryption)

II] Asymmetric Encryption

Asymmetric encryption is the other kind of encryption in which two keys are used. To give an explanation for greater, what Key1 can encrypt only Key2 can decrypt, and vice versa. It is also known as Public Key Cryptography (PKC), because users generally tend to use keys: public key, which is understood to the general public, and private key which is thought most effective to the user. Figure five below illustrates the use of the 2 keys among node A and node B. After agreeing on the sort of encryption for use inside the connection, node B sends its public key to node A. Node A uses the obtained public key to encrypt its messages. Then when the encrypted messages arrive, node B makes use of its non-public key to decrypt them.

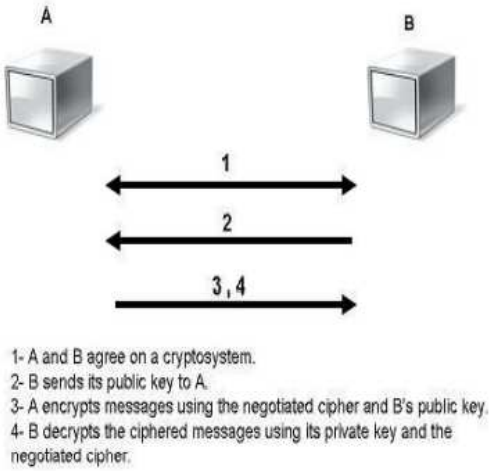

Fig 7(Asymmetric encryption)

3. Conclusion

The RSA encryption set of rules is presents high records protection and excessive control congestion among customers and sever because server is utilized by more than one user. The non-public key's despatched to the consumer mail account. Based on the private key and public key, the record is view and downloads from the cloud. In this work, this permits for an awful lot more green computing by

centralizing storage, reminiscence, processing and bandwidth. The proposed set of rules is very assisting complete to increase the overall performance in cloud computing.

The proposed key management has taken into consideration various parameters for the identity of the precise key mechanism which is suitable for providing the desired security. The key control capabilities have considered protection, rapid transmission of data and each and every key has one-of-a-kind functionalities but embedding them in a single key characteristic produce favoured effects. The customer keeping the appropriate than provider.

Securing the garage of encryption keys will subsequently lessen the attacks from intruders, viruses and other forms. This has centred on specific ideas of cryptography related encryption keys and relaxed storage of encryption keys.

Different types of garage devices and not unusual attacks on them are studied which helped us in presenting a secure system for garage of encryption keys. Finally securing encryption keys is a tough venture. By using some third birthday celebration tools in the device which presents administrator manage, we can gain such comfortable storage.

This describes the studies historical past of securing statistics inside the garage and provide out the layout criteria of treatment storage systems. To make the studies popularity be more without difficulty understood, we extract the important thing technologies which might be adopted in the current comfy storage systems, classify the technology into one-of-a-kind classes, and discuss their deserves and weaknesses. Based on cloud storage, the new garage form which has drawn lots interest recently, we additionally gift the challenges of protection inside the cloud storage environment. Finally, we conclude and provide the assessment of numerous traditional storage structures.

The cloud computing structure shops statistics and alertness software program with minimum management effort and presents on call for services to customers thru internet. But with cloud control consumer don't have trust worth commitments or regulations. This will lead to many protection problems with records garage consisting of privateness, confidentiality, integrity and availability. In this observe we targeted on records garage security troubles in cloud computing and we first supplied service models of cloud, deployment models and form of safety issues in data storage in cloud environment. In the very last segment, we addressed viable answers for the information storage problems that provide privateness and confidentiality in cloud environment.

References

[1] P. k. V and v. Vijayakumar, "Survey on the Key Management for securing the Cloud," *Procedia Computer Science,* 2015.

[2] V. K. Damera, D. S. Pabboju and P. S. Sunder, "Secure Storage of Encryption Keys," *International Journal of Engineering Research & Technology (IJERT),* 2012.

[3] J. Shu, . Z. Shen, W. Xue and . Y. Fu, "Secure storage system and key technologies," *researchgate.net,* 2013.

[4] O. Stephen, "The Study of the Application of Data Encryption," *International Journal of Scientific and Research Publications,* 2014.

[5] P. Yellamma, D. C. Narasimham and D. B. SubbaRao, "Data Security f ta Security for Cloud Using Pub or Cloud Using Public Key," *researchgate.net,* 2016.

[6] A. Alrehaili, A. Mir and J. Mir, "A Retrospect of Prominent Cloud Security," *International Journal of Innovative Technology and Exploring Engineering (IJITEE),* 2020.

[7] N. vurukonda and B. Rao, "A Study on Data Storage Security Issues in Cloud Computing," *Procedia Computer Science,* 2016.

[8] E. Goh, H. Shacham, N. Modadugu and D. Boneh, "SiRiUS: Securing Remote Untrusted Storage," *NDSS,* 2003.

[9] E. Geron and A. . Wool, "CRUST: Cryptographic remote untrusted storage without public keys," *IEEE,* 2007.

[10] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang and K. Fu, " Plutus-Scalable secure file sharing on untrusted storage," *FAST,* 2003.

[11] M. Chase, "Multi-authority attribute based encryption," *Lecture Notes in Computer science,* 2007.

[12] A. Adya, W. Bolosky, M. Castro, G. Celmak, R. Chaiken, J. Douceur, J. Howell, J. Lorch, M. Theimer and R. Wattenhofer, "FARSITE: Federated,available, and reliable storage for an incompletely trusted environment.," *OSDI,* 2002.

[13] P. Stanton, "Securing Data in Storage: A Review of Current Research," *CORR,* 2004.

[14] A. Singh and L. Liu, "SHAROES: A Data Sharing Platform for Out-sourced Enterprise Storage Environments," *ICDE,* 2008.

[15] J. Li, M. Krohn, D. Mazi`eres and D. Shasha, "Secure Untrusted DataRepository(SUNDR)," *OSDI,* 2004.

[16] P. Ahmed and e. al, "An intrusion detection and prevention system in cloud computing: A systematic review," *Journal of Network and Computer Applications,* 2013.

[17] Reddy, V. Krishna, B. T. Rao and S. S. R. L, "Research issues in cloud computing.," *Global Journal of Computer Science and Technology,* 2011.

[18] S. Singh, Y. Jeong and J. Park, "A survey on cloud computing security: Issues, threats, and solutions,," *JOURNAL OF NETWORK AND COMPUTER APPLICATIONS,* 2016.

[19] A. Tripathi and A. Mishra, ""Cloud Computing Security Considerations," *IEEE,* 2011.

[20] A. Bouayad, "Cloud Computing: Security Challenges," *IEEE,* 2012.