Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 10021 - 10027
Received 05 March 2021; Accepted 01 April 2021.

Exploiting Code Generation and Belief Propagation to Infer Identity of Polluters in Cloud Environment

M. Robinson Joel[1],V.Ebenezer[2], K.Arul Jeyaraj[3], K.Rajkumar[3],M.Varghese[4], [1]E.Bijolin Edwin

[1]Ponnaiyah Ramajayam Institute of Science and Technology, (PRIST),Chennai,India.
[2]Karunya Institute of Technology and Sciences, Coimbatore, India.
[3]PSNA College of Engineering and Technology, Dindigul, India.
[4]PSN College of Engineering and Technology, Tirunelveli, India.
ebenezer88@gmail.com

ABSTRACT

In today's, digital world the usage of new technology has increased tremendously. Nowadays, the confidentiality of our data which we send or store for our privacy purpose is not completely secured and protected. It's because of digitalized thefts like Brute Force attack, corruption of data, cloud storage data thereafter etc. In order to overcome these thefts and secure our data, I have proposed a web application security using RKG and Belief Propagation algorithm. Here, we can able to secure the data even in cloud storage system. Using these algorithms, detection of corrupt data, password thereafter has been done and the data is secured and protected in this web application security.

KEYWORDS: RKG algorithm, Belief Propagation algorithm, Brute Force attack, Security.

1.INTRODUCTION

In today's digital world there are so many intruders trying to hack our data in cloud storage also like injecting some malicious script so far to avoid that kind of issues. so In the cloud storage also we are protecting our data's for example (on that time if a cloud data owner is sending a file means we doesn't know if there any malicious script injected in our data are not. To check that type of issues we are using a method called(DPI) deep packet inspection it will analyze all the fragments except the header information. To check that there is any malicious script injected on file or not if there no any malicious script means the file will send to the server. if the (DPI FILE) detected any malicious script means they file will not send to the server it will block the IP(address). In the web application, we are using two types of algorithms there are namely RKG and BPCORE.To share and access configurable resources like applications, services, storage, servers and computer networks through some minimum effort over the internet are modelled as Cloud computing information Technology. The enterprises and the users are retrieving and storing large data using numerous computing facilities available. They are doing this on the data center server managed by third-party and private-owned cloud storage which make the accessing method easy. These Cloud computing concepts minimize the cost of storage amount spend by the information technology for maintaining and storage space for their organization. Here the third-party cloud storage plays an important role in minimizing the economy and utilization of data.During 2013 they submit a report regarding the service and maximum usage because of the fast performance of the Cloud, good accessibility, scalability and also more availability. Cloud computing storage increases and lead to an increase in the vendor side also. Cloud vendors also increase double the amount compared in the last decade. Even though vendors and cloud storage increases there is some drawback in the service and user-friendly session.

In the mid of 2009, the growth of Cloud computing increase due to growth of storage needed, growth of high-speed networks, computer cost decrease and service-oriented architecture. Joel[2] and his team explained the different cloud storage providers and their maximum capacities of storage available as free of cost.The architecture of Cloud computing contains many components which help them to transfer and storage the mass storage of data. As a front-end component, the client infrastructure role is very important in contact with the cloud to the customer node. In the architecture phase, the application that they are using to connect and the service they provided are very important. In the following, we can see the different types of service providers.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 10021 - 10027
Received 05 March 2021; Accepted 01 April 2021.

SaaS is the services of cloud application that act on the web browser directly which means we do not require to download and install these applications. Google apps and hubspot are some examples.

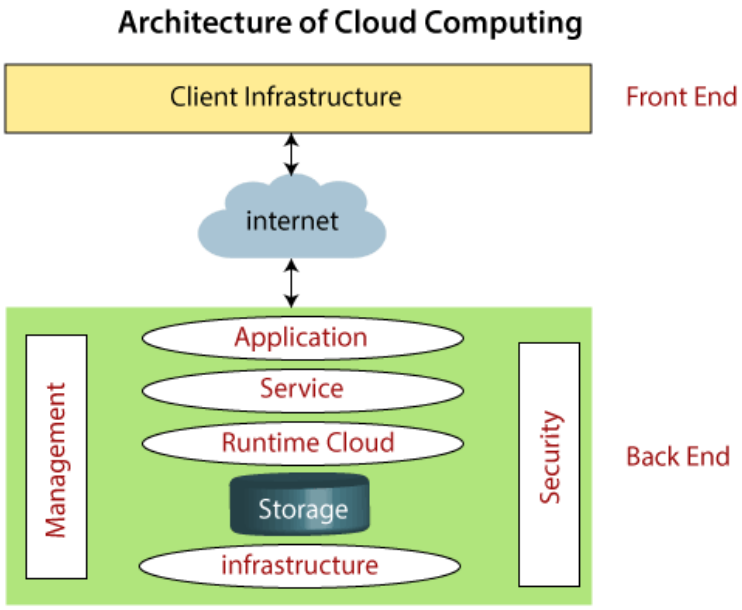

Figure 1. Cloud architecture

Paas is termed as cloud platform services also similar to SaaS, but the main difference is that PaaS may support or provides a platform that is also used to create software. Examples are Windows Azure, Force.com, Magento Commerce Cloud[17][18][19][20].

2. RELATED WORK

In this section, we can go through many proposed works suggested by researchers. Let us go through one by one in details before going to our proposed work. In wireless networks, there are many securing routing protocols used to establish and maintain packet forwarding with full security. For the route selection process, they establish many Secure route establishment [7][3][4], which secure from attacker attack the nodes. For packet forwarding process they implement pollution attacks but the secure route establishment comes as a substitute for this also. R. Curtmola explained about the packet injection and similarly the dropping attacks related to secure packet forwarding [5][6][1]. These packet injections designed for old methods of the routing protocol.

2.1. RKG algorithm

RKG technique is an event-based OTP, whenever a brute force attack is been detected an random OTP is sent to the authorized user e-mail address. RKG technique is used to generate one time passwords based authentication to avoid password thefts. The user then authenticates with OTP himself with OTP. The OTP is checked at the server and the transaction proceeds if valid Joel[2] explained details about cloud storage and security issues.

2.2. BPCORE algorithm

BP Core algorithm is used to identify the polluters in the system. During the polluter's identification stage, the Proxy checking before the firewall gathers all the n fragments and checks for malicious code.

Belief Propagation (BP) that has been already applied to the problem of polluter identification in the different scenario during data transmission. BP Core algorithm helps to decide on the most likely polluter and honest node, respectively. Doing plaintext and make a key as inputs and create a text as cipher text is termed as

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 10021 - 10027
Received 05 March 2021; Accepted 01 April 2021.

Enciphering. Similarly, vice-versa is termed as deciphering where it takes cipher text along with key as input and produce the plain text as output. As of the authors proposed in the [8] and [9], the symmetric cryptography system there only one key is used as the secret key for both locking and unlocking the text that is encryption and decryption between two nodes. One time password encryption method is one of the best encryption algorithms nowadays used to do the transaction. Its is an enhanced application of Vigenere cryptosystem [10] that do some modification in the length of the key generation.Lehmer [11] proposed this algorithm as LCG method. They utilize the simple way by using the formula

$$g(n+1) = (k.g(n)+c) \bmod p \quad (1)$$

where c, p, and k are positive non-zero constants, and g(n + 1) is calculated iteratively. g(n) is the seed number that is the first part of random key.M. Sokouti [12] have proposed an improved version of the key generation of the stream cipher. They conducted the trial on an average of 10 random keys in 90 tests. They completed reviewed and also does discussed chromosomes and population in 100 generations. They also compared with the 10P-GRKG algorithm and shows that they cover the drawbacks of 10P-GRKG method. Their proposed system has a seven-parameter key and decreasing the parameters of the key from 10 to 7 is one of our approaches.

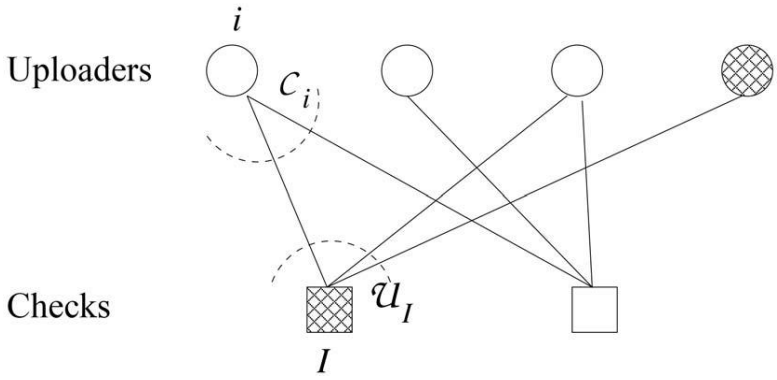

Figure 2. Bipartite graph

Rossano Gaeta [16] proposed a method that in MANET nodes disseminates data using the codes. He proposed SIEVE, where they can identify the malicious code in a distributed way. When a chunk is decoded Rossano Gaeta named it as check as it is pair of composed of another set of nodes which provide coded blocks used to decode the chunk. It indicates whether the chunk is corrupted with a flag indicator.To detect chunk integrity SIEVE exploits a code and even to identify they use beliefpropagation[14][15]. Here the node constructs it's a graph as shown in Figure 2where the vertexes are checks and nodes.

3.PROPOSED ALGORITHM

The proposed system consists of two algorithms namely random key generation and Belief Propagation algorithm. The random key generation is used to create the One Time Password and the Belief Propagation used to clear the nodes. The below architecture Figure 3 shows, how the flow of transaction taking place. In our proposed system we are using the improved genetic-based random key generator (IGRKG). In this, they are using LeastGen variable parameter and short key generated compared to other key generators. This belief propagation does the identification of malicious nodes from the set of checks.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 10021 - 10027
Received 05 March 2021; Accepted 01 April 2021.

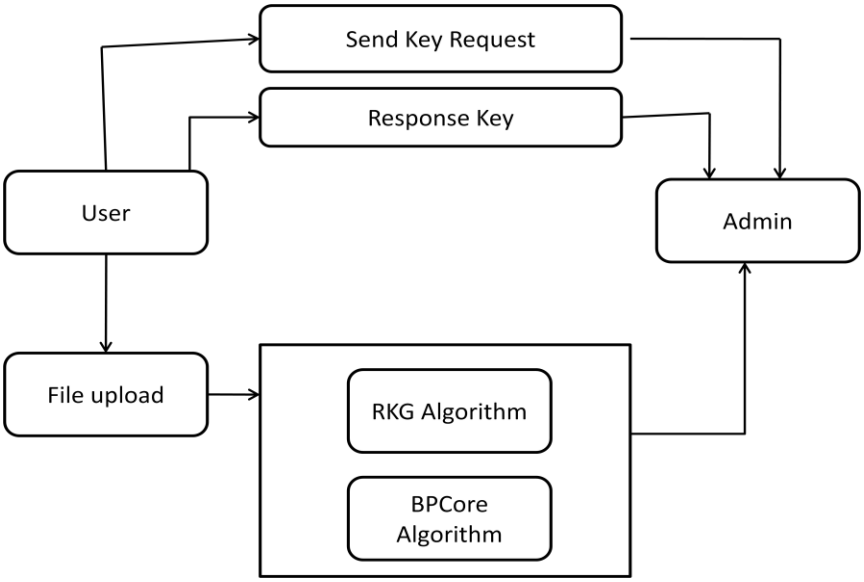

Figure 3. File upload using the algorithm architecture

When the user wants to upload a file, it will get permission from the admin by sending request. When the admin accepts the request, he will send a acknowledge message to the user. Now the file will be upload by creating two algorithms as mention early. From the user side and admin side also, they send the encrypted key to activate the response and return of the messages.

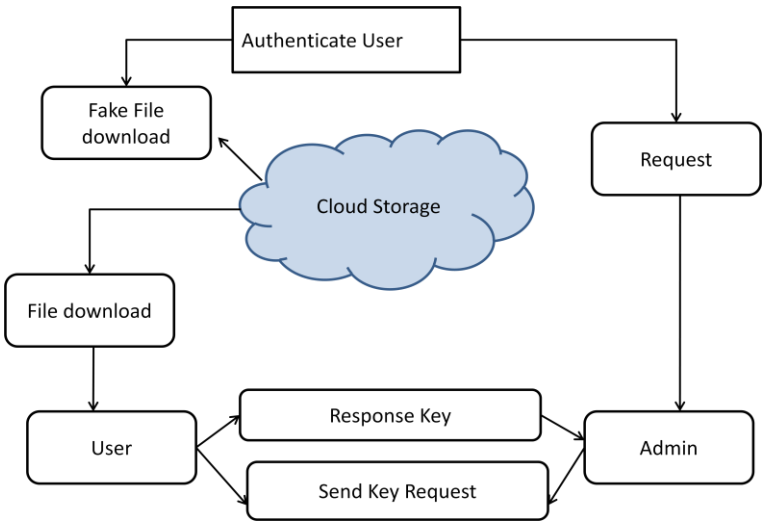

Figure 4. File download using the user authenticate architecture

When the user wants to download a file, it will get permission from the admin by sending request. When the admin accepts the request, he will send a acknowledge message to the user. Now the file will be download. Figure 4shows the architecture of the download process. Here from the cloud, there are possibilities that the fake documents also downloaded. To avoid these, we are using the same algorithm to do security issues.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 10021 - 10027
Received 05 March 2021; Accepted 01 April 2021.

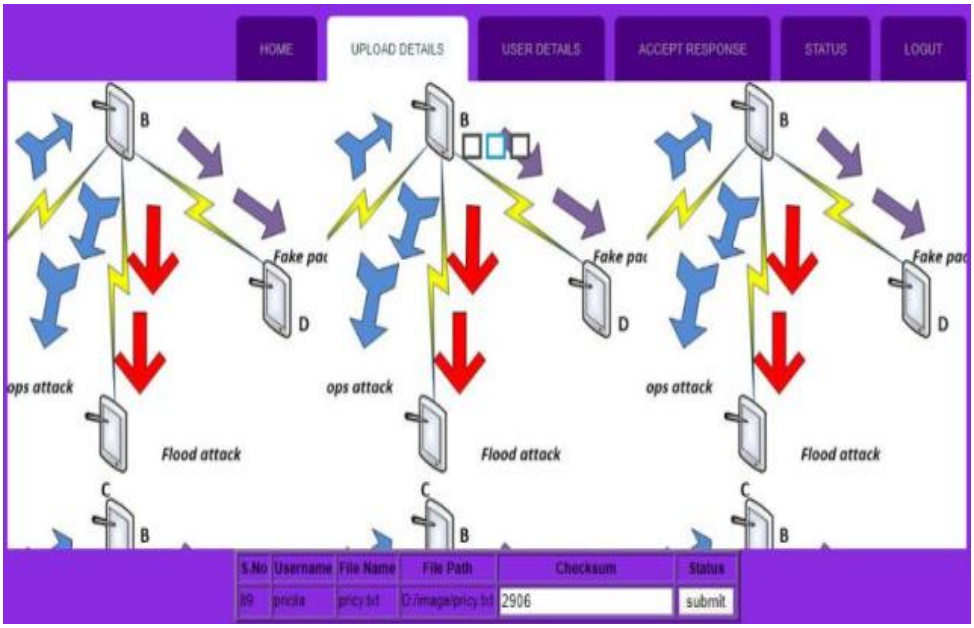

Figure 5. Checksum upload

The screenshot shows Figure 5 the checksums of the uploaded file, also user name and the file name. Now the file will be upload by creating two algorithms as mention early. From the user side and admin side also, they send the encrypted key to activate the response and return of the messages.

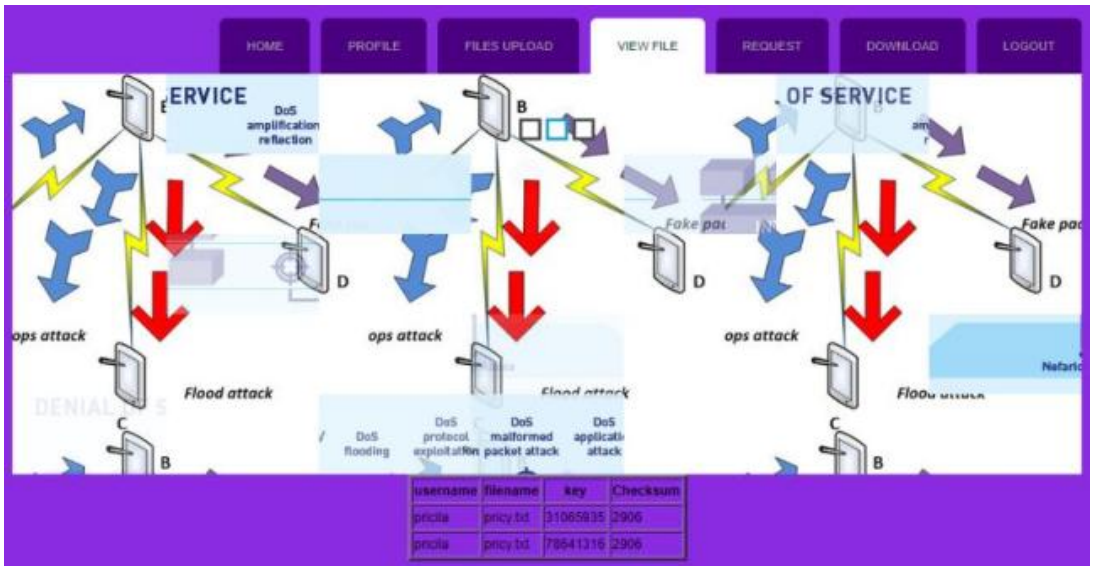

Figure 6. Shows the download details

When the user wants to download a file, it will get permission from the admin by sending request. The screenshot shows Figure 6 the checksums of the downloaded file, also the user name and the file name.

4. CONCLUSION

This proposed system addresses in preserving user data confidentiality and integrity after outsourcing. In this work, the mechanism for pollution detection is to check the data security when we try to upload and download the file. This paper also identifies malicious nodes and finds the fake file. In order to overcome the thefts and

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 10021 - 10027
Received 05 March 2021; Accepted 01 April 2021.

secure our data, this paper proposed a web application security using RKG and Belief Propagation algorithm. Here, we can able to secure the data even in cloud storage system. Future work can focus on the finding of the malicious file or node and kill that file from the storage network.

REFERENCES

[1] J. Dong, R. Curtmola, & C. Nita-Rotaru (2008), "On the pitfalls of using high throughput multicast metrics in adversarial wireless mesh networks", in Proc. of SECON '08.

[2] M.Robinson Joel, M.NavaneethakrishnanT.D.JebaFreeda&R.Arunadevi, (2020), "An Analysis On Storage And Security Over Cloud Platform", International journal of analytical and experimental modal analysis, vol. 12, no.1, pp.2222-2226.

[3] Y.-C. Hu, D. B. Johnson, &A. Perrig, (2002) "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks", in WMCSA.

[4] M. Guerrero Zapata & N. Asokan, (2002), Securing Ad hoc Routing Protocols, in WiSe,

[5] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, & H. Rubens, (2008), ODSBR: "An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks", ACM Trans. Inf. Syst. Secur.,

[6] R. Curtmola& C. Nita-Rotaru, (2007). BSMR: Byzantine-resilient secure multicast routing in multi-hop wireless networks, in SECON,

[7] Y.-C. Hu, A. Perrig, &D. B. Johnson, (2005), Ariadne: a secure on-demand routing protocol for ad hoc networks, Wireless. Networks., --------

[8] Bagnall AJ, (1996), The applications of genetic algorithms in Cryptanalysis, MSc thesis, School of Information Systems, University of East Anglia.

[9] Schroeder, (2008), Number theory in science and communication: with applications in cryptography, physics, digital information, computing, and self-similarity, Springer, New York.

[10] Sokouti M&Sokouti B, (2009), Improved version of Vigenere algorithm, 12th conference of ISCEE, Tabriz-Iran, pp.13–15.

[11] Stallings W, (2002). Cryptography and network security: principles and practice, 3/e, Prentice Hall,

[12] M. Sokouti, B. Sokouti, S. Pashazadeh, M.-R. Feizi-Derakhshi, &S. Haghipour, (2013), Genetic-based random key generator (GRKG): A new method for generating more-random keys for one-time pad cryptosystem,Neural Computing and Applications, 22 (7), pp. 1667–1675.

[13] D. MacKay, (2003), Information Theory, Inference and Learning Algorithms. Cambridge, U.K.: Cambridge University Press.

[14] J. Yedidia, W. Freeman, & Y. Weiss, (2005), "Constructing free-energy approximations and generalized belief propagation algorithm", IEEE Transactions of Information Theory, vol. 51, no. 7, pp. 2282–2312.

[15] J. Yedidia, W. Freeman, & Y. Weiss, (2003). Understanding belief propagation and its generalizations, Exploring Artificial Intelligence in the New Millennium, San Francisco, CA, USA: Elsevier,

[16] R. Gaeta, M. Grangetto& R. Loti, (2014), "Exploiting Rateless Codes and Belief Propagation to Infer Identity of Polluters in MANET", IEEE Transactions on Mobile Computing, vol. 13, no. 7, pp. 1482-1494.

[17] V. Sakthivelmurugan, R. Vimala, &K.R. AravindBritto, (2018), Magnum opus of an efficient hospitality technique for loadbalancing in cloud environment. Concurrency Comput. Prac. Exp. Vol. 31, no. 14, pp.1–11.

[18] V. Sakthivelmurugan, R. Vimala, &K. Rajkumar, (2017), "Thershold max method for load balancing incloud computing". Asian. Journal of Res. Soc. Sci. Humanit, vol. 7, no.2, pp.640–650.

[19] V. Sakthivelmurugan, R. Vimala, &K.R. AravindBritto, (2019), "Star hotel hospitality load balancing technique in cloud computing environment". Adv. Intell. Syst. Computvol. 750, pp.119–126.

[20] Krishnan Rajkumar, A. Sangeetha, V. Ebenezer, G. Ramesh, & N. Karthik, (2021), "Designing Parallel Operation for High-Performance Cloud Computing Using Partition Algorithm",Advances in Intelligent Systems and Computing, vol. 1167 pp.451-462.