Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7 July 2021: 12402 – 12407

Research Article

Privacy Preserving Protocol for Intercloud

S.Sreeram[1], Dr.Ashok kumar[2]

Abstract

Cloud computing plays a vital role in the field of information security. Many numerous data's are stored in cloud. Resource sharing plays a keen importance in data sharing. When sharing the data the datas which we are going to send should be in an encrypted form so that if any hacker tries to hack the data which he got cannot be used by him. Many protocols have been used to preserve the data as encryption in data sharing. For this encryption system only we are going to propose the concept of trust evaluation protocol. Certain steps are been followed to build up this protocol. First the feedback will be taken separately and it will be encrypted and secondly we have to classify the nature of intercloud activity. Then at last we will introduce the new scheme of trust evaluation protocol which will help in safe guarding the data's that we are going to share in the cloud storage.

Keywords- Encryption, Decryption, Transmission rate, Delivery ratio, Intercloud.

I INTRODUCTION

Most of the data gets stored in the server the server which is nothing but the database. The database or highly confidential which can have all the customers details in a one particular place. The data are in the encrypted from when there is any need of the data it is get decrypted and then used in the webpage. Likewise big corporate like Google they can maintain a huge database millions of customers are using the Google server. It is the world's biggest

Server when compared to others these server are highly secured and cannot by hacked by anyone.

But other than these site there are large number of local site such as shopping site, food site likewise. They are secured but it can be easily hacked by anyone. To avoid these problem in these paper they proposes a new technique which is the pettifog system. By using this it made the system so secured and safe. Before the data we provided is going to the server a several steps have to made to maintain the data secured. The data is first given in the website by the customer is first collected in the local host after that the masking is provided to the data. To make the data so safe. After the masking the data gets separated and allocated a different storage path in the

[1]UG Scholar, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India
[2]Assistant Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India. E-mail: sreerampk36@gmail.com

server. Because the data of the one particular person in allocated at the same place it is easily to hack the data by the hackers. So the address of the data can varies and the fetching of the data can be avoided. The maximum process has been completed. Next stage is the firewall stage in which the data can be surrounded numerous firewalls. The pettifog algorithm has been used which can makes the data so safe and protect them from the hacking of original content. The data which is the local host can be moved to the database. Now the data become more safe and it cannot occupied by any of the third party member. The SQL inoculation system is implemented which act as anti-theft tool to the data of the persons who are all using the website. Each website has the server and the server can be monitored by the technical team. Even though the monitoring lakhs of people can entering and relieving the web which they can including the data. So it is difficult to monitor using the man power. This inoculation can provide the data and act as the security guard to safeguard all the bio data and the bank section. The details can be separated at various part of section the section can be separated at various part in the database. Each section has the separate address. The address can be gets stored in the web. When the particular person login the details get fetched together and displayed in the screen. For each customers the data can be separated the distributed data can be gathered and displayed in the system page. This system is more secured.

II LITERATURE SURVEY

Jayaram Pradhan et., al., proposed the data communicates through the network layer from the transmitter to receiver. In WSN the security is not much effective. The data transfer between the nodes is highly efficient. Due to the lack of security in the communication path. The hackers can easily enter the main section by attacking the various layer of protocols in WSN. The AODV system faces the security issues when the discovery process took place. So the users get fear to use the network layer for the communication. In this paper they propose the NL-IDS system. In which it can detects the black hole of the person who fetching the data from the nodes. The node trust of the sensor layer can be calculated based upon the black holes. The watchdog timer is used to calculate the deviation of the each node at specific period of time. The overall deviation can be calculated to find out the average value. Each node can carry the past and the present data. The NL-IDS system can easily find out the affected node and it get replaced by the other node. The node can carry the information of the next node. The simulation can be made using the MATLAB to calculate the NL-IDS. This method can gives the high accuracy and efficiency with false alarm rate. [1]

Colin C. Murphy et., al., proposed the internet can plays a vital role in the every person life. All the confidential data can be handling in the internet. The data are getting stored in the database. The data can be easily hacked by the unauthorized person or by the hackers. The Internet of things which can plays the major role in the network part. The data can be uploaded and viewed in the IOT. The data can be transferred through the node. The router has the several nodes, the nodes are get interlinked to form the communication network. Hackers can create a malicious data pack at the neighborhood node. The data can be attacked by the malicious data pack. To avoid the hacking of the data in this paper they proposes the COTS devices which act as the communication protocol in which the data transfer can be made more confidential manner. The data in the path is more standard in which can be undetected by the hackers. The WSN which use the particular protocol for the data extracting if the protocol does not match it detects the

malicious data. In further the ZIGBEE based data transmission it can communicate the data at fast rate. The ZIGBEE can be interlinked with ISM which can act as the head of the network. The COTS devices are installed to detect the malicious data in the node connection. [2]

Haruo Yokota et., al., proposed in wireless sensor network the data communication can made through the node to node transfer. Using the nodes the hackers can creates the malicious data in each node when the data reaches the node it subjected to the malicious attack. It can create a uncertainty condition and it affects the environment by creating false alarm. To avoid these problems in this paper they proposes the detecting of the abnormal node. The abnormal node can be detected by using two methods spatial temporal ST and multivariate attribute MVA of sensor correlations. The ST sensor data are get gathered in the separate medium and it makes cross comparison is made between the node streams and the sensors. The threshold value is compared with the cross comparison. The MVA data and the ST cross comparison data can be interlinked together to reduce the abnormal nodes. This method can avoid the false alarm system can safeguard the node data from the malicious attack. The data can be in the standardized path. So the unauthorized person cannot able to create a attack in the node path to fetches the data. [3]

Houbing Song et., al., proposed when compared to the other network system the wireless sensor network WSN which has the lack of security. Data communication can be made through the communication protocols. As the WSN system implied the use of various protocols can be increased. The increased protocols are mainly for the security purpose. These protocols can make the network layer more complex and it consume high amount of energy. To avoid this kind of problems in this paper they propose the knowledge based context aware approach. It can detect the malicious nodes present in the network layer. In the network layer knowledge based is in the base station, the knowledge based can accumulate all the data of the nodes. Nodes are connected in the form of cluster, the cluster head node which can block the malicious nodes in which data repetition appeared. Base station can affect the network layer this can be avoided by minimizing the security protection. [4]

Nei Kato et., al., proposed the WSN can extended the application in the field of the medical. The sensor can be setup in the body in which can reads the body parameters of the patient regularly. The sensed data whose resources are get limited. Environmental condition and the malicious attack can create a false data in which the false alarm is generated. If the false data of the patient can be transfer to the doctor, so based upon the false data the treatment is made which can affects the health of the patient. To make the WSN safe and secured in this paper they proposes the Bayesian network model based sensor network in which can prevents the data attack by the malicious node. This method can reads the training sets of the sensor data it can make the system process more accurate. The collection all the sensor data is avoided in this method. It can avoid the inaccuracy of data. The data base is maintained in which they collects the all the false alarm generated in the process. The number of false alarm generated is calculated and the performance is compared with the other methods. It can provide the better accuracy. [5]

Sunho Lim et., al., proposed the WSN has the lack of security in the physical protection and the co-ordination. The network protocols can be easily hacked by the unauthorized person. The DOS attack which is the denial of service attack which can affect the main server of the network layer or the current data communication path to fetches the data. To make the network layer more

secured in this paper they propose the SCAD method. The SCAD can create check point in the communication between each nodes. The checkpoints are counter measured for the forward data transfer technique. The checkpoint can detect the malicious node in the network layer The simulation has been made to detect the performance by using the countermeasure technique the PDR can be detected which is the packet delivery ratio. The consumption of the energy is less compared to the other safety methods. The accuracy can be increased by the use of the counter measure. [6]

G.S Binu et., al., proposed compared to the wired sensor network, the wireless sensor network is not much secured due to the lack of security. The WSN can extend the application in the traffic monitoring, military. Due to the security defects they are not much used in these fields. The data is broadcast at the time of transmission the attackers can create the security nodes can fetches the data. Selective forwarding attack can target the network layer can stops the traveling of the data forwarding, the data leakage can occurs at the place. In this paper they propose the energy efficient detection algorithm which can detect the forward attacking of the data packets. This method can provide the accurate data security. The checkpoint can detect the malicious node in the network layer The simulation has been made to detect the performance by using the countermeasure technique the PDR can be detected which is the packet delivery ratio. Malicious node can be detected in the network layer with the help of the energy efficient algorithm. It consumes less amount of power. The false alarm is reduced and the value is get recorded in the database. [7]

M. Rajesh et., al., proposed WSN can be applied in the field of the border security, radar surveillance etc., For the border security applications the data security in the network communication is more important. There are several types of attack to fetches the data in the communication layer. The false injection attack can attack the nodes of the data it is the dangerous attack in the network protocol. RSS, ECC are employed for the prevention of the false data injection in the communication path. The paper proposes the trusted parameter it can separate the node into two different mode malicious node and the non malicious node. The non malicious node can be used in the forward data transmission packet to the server. The simulation is made in the NS2 and energy consumption is also minimum. [8]

Donghui Li et., al., proposed Easy attack by the environment conditions, consumption of power, poor hardware constructions and the lack of security data. These drawbacks in the WSN can be overcome with implementing the paper. This paper proposes the novel trust routing protocol method it gathers the number of attributes of the sensor network such as the energy, data, and communication. The use the sliding window method to detect the malicious node in the network layer. The nodes can be interlinked to from the communication to secure the information in the path by use of this method. The time consumption can be reduced up to 7% and the data packets can be increased up to 12%. [9]

Guruprasanna et., al., proposed the MANET which is the mobile ad-hoc network it has the various node for the data transfer. The malicious node are get created and attack the data in the other nodes. So to detect the malicious node in this paper they proposes the CBDS method which is the co-operate in active bait discovery method which use the Reverse mapping technique to

create a effective to route to transfer the data from the node to the target and it avoid the data loss. Establishment of route can be made by the Dynamic source routing scheme.

III PROPSED METHOD OF PRIVACY PRESERVING

In this paper they show about the preserving of the data of one's own data in cloud sharing and storage. They can preserve the data of the all the members in the cloud. This paper proposes the trust worthy evaluation method in which it act as the security barrier to prevent the extraction of the data by the unauthorized person.

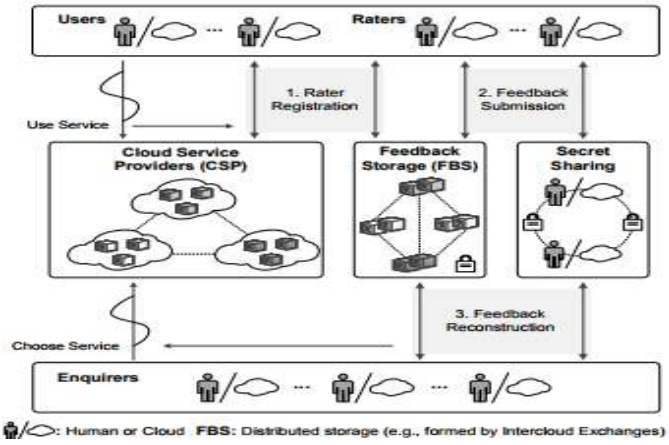
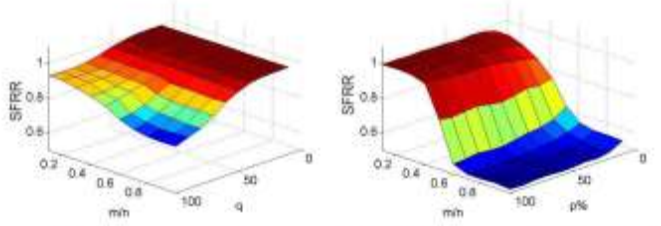


Figure 1: System Architecture

IV RESULTS AND DISCUSSIONS

In our proposed system we are going to develop a new trust evaluation protocol. All the data's feedback that we are going to share will be taken separately and encryption takes place. Secondly the nature of activity of the intercloud is classified. According to the nature of activity the data's that are going to be shared will be tabulated. At last our proposed system of giving trust worthy in the data's that are going to be shared takes place resulting in good accuracy in safeguarding the data's from attacks.



(a) Random-a, $q \in [10, 100]$. (b) Random-b, $p \in [10\%, 100\%]$

Figure 2: Effect of increasing m/n ratio on successful feedback recovery rate (SFRR)

V CONCLUSION

Preserving data's is very important in cloud storage. Data has to be maintained well and has to be compulsorily been safe guarded as many hacking is taking place occasionally. Our proposed system will help in improving the encryption process in safe guarding the data's. It is proved that the accuracy in preserving the data is more than 90 percentages.

REFERENCES

[1] Chaudhuri, K.; Monteleoni, C.; and Sarwate, A. D. 2011. Differentially private empirical risk minimization. Journal of Machine Learning Research 12(3):1069–1109.
[2] Dwork, C.; McSherry, F.; Nissim, K.; and Smith, A. 2006. Calibrating noise to sensitivity in private data analysis. In TCC, 265–284.
[3] Fredrikson, M.; Lantz, E.; Jha, S.; Lin, S.; Page, D.; and Ristenpart, T. 2014. Privacy in pharmacogenetics: An end-toend case study of personalized warfarin dosing. In USENIX, 17–32.
[4] Fredrikson, M.; Jha, S.; and Ristenpart, T. 2015. Model inversion attacks that exploit confidence information and basic countermeasures. In CCS, 1322–1333.
[5] Hoens, T. R.; Blanton, M.; and Chawla, N. V. 2010. A private and reliable recommendation system for social networks. In SocialCom, 816–825.
[6] Hua, J.; Xia, C.; and Zhong, S. 2015. Differentially private matrix factorization. In IJCAI, 1763–1770.
[7] Jorgensen, Z., and Yu, T. 2014. A privacy- preserving framework for personalized, social recommendations. In EDBT, 571–582.
[8] Komarova, T.; Nekipelov, D.; and Yakovlev, E. 2013. Estimation of treatment effects from combined data: Identification versus data security. In Iccas-Sice, 3066–3071.
[9] Koren, Y.; Bell, R. M.; and Volinsky, C. 2009. Matrix factorization techniques for recommender systems. IEEE Computer 42(8):30–37.
[10] Koren, Y. 2008. Factorization meets the neighborhood: a multifaceted collaborative filtering model. In SIGKDD, 426–434.