AN EFFICIENT DISASTER RECOVERY APPROACH IN CLOUD WITH SECURE ENCRYPTION

Dr.S.Subashree.M.E.,Ph.D (Guide)
K.Aarthi, B.Yogalakshmi
E.G.S.Pillay Engineering College, Nagapattinam.
An Autonomous Institution; Affiliated To
Anna University: Chennai 600 025

ABSTRACT

Cloud computing is considered as a possible way to lower the cost and complexity of computing by furnishing operations running on the Internet. numerous associations and business models are looking at Cloud computing as a new form of exigency operation which will keep business durability.Cloud computing could contribute to exigency operation since it could grease the sharing of information among private and government associations. A system for system resource operation of a Cloud Computing-grounded disaster recovery is proposed. This system can determine whether system performance achieves the “ recovery point ideal ”(RPO) or not. It's also necessary to resize coffers for satisfying needed performance at lower cost. thus, a formula for bluffing system performance is established. It's important to consider data vacuity, backups and redundancy as element of the exigency operation software selection process. This is especially important in case of a natural disaster where there's a high threat of losing access to computers and data centre. The data should be constantly backed up and stored in multiple locales separated by enough distance depending on the type of the disaster. Disasters similar as fires, cataracts and earthquakes are more indigenous, while hurricanes can affect entire seacoast lines. It's important that the primary and provisory spots are geographically separated in order to insure that a single disaster won't impact both spots. A secure encryption system is handed to cipher the lines. RSA encryption system was employed for cipher the lines also the translated lines are stored on garçon. This type of encryption process is provides further secure way for train transferring and recovering process. This proposed work has following modules.

Keyword: Recovery Point ideal ,RSA,Disaster,Cloud Computing

INTRODUCTION

Cloud-based disaster recovery has grown to be widely used in many field due to its range of positive aspects. Since the disaster recovery is present within a cloud, it minimizes the actual up-front capital costs. In the situation of disaster data management, Big Data indicates the enormous bunch of datasets produced through different individuals and also consists of different data structures, which includes structured, semi-structured, and unstructured data. Furthermore, every inability within software or hardware could potentially disrupt the actual work-flows or data and therefore, would certainly threat the customers. Consequently, Big Data come with an essential demand to add deployment of a disaster recovery plan to guarantee safe sources of data. Businesses are subjected to threats that can interrupt operations, disaffect clients and also endanger company trustworthiness as well as income avenues. Threat can even be exposed to an organization by changes. Data is incredibly beneficial business resource, the data is essential for businesses, particularly highly dependent on the data of businesses.

When a system crashes or power failure occurs there is a chance of loss of data and sometimes it may result it in financial loss. This system crashing and other problems occur due to natural Disasters or by anthropomorphous from causing expensive service disruptions. When a disaster come in business continuity the company may get large loss of data and also financial loss. When disaster occurs company need to protect the data from loss. Cloud providing companies like Google, Amazon, Microsoft etc., experienced cloud disaster with a huge loss of data and servers. When disaster fall out at client side backup will be stored in cloud but if disaster occurs in cloud data will be lost. Natural disasters may occur due to bad weather results in disaster. To overcome these disasters there are some disaster recovery techniques which are used to recover data.

Disaster recovery techniques as necessary to their business continuity. Dedicated and shared models are the two approaches for disaster recovery based on cost and speed. Storing the data from cloud infrastructure in order to recover when disaster occur. Every organization should have a documented disaster recovery noesis and should test that process at least twice each year.

LITERATURE SURVEY

1. Zheng, Jing, Qi Li, GuofeiGu, Jiahao Cao, David KY Yau, and Jianping Wu. "RealtimeDDoSdefense using COTS SDN switches via adaptive correlation analysis." IEEE Transactions on Information Forensics and Security 13, no. 7 (2018): 1838-1853.

   In this paper, we propose RADAR to detect and throttle DDoS attacks via adaptive correlation analysis built upon unmodified commercial off-the-shelf (COTS) SDN switches. It is a practical system to defend against a wide range of flooding-based DDoS attacks, e.g., link flooding (including Crossfire), SYN flooding, and UDP-based amplification attacks, while requiring neither modifications in SDN switches/protocols nor extra appliances. It accurately detects attacks by identifying attack features in suspicious flows, and locates attackers (or victims) to throttle the attack traffic by adaptive correlation analysis. We implement RADAR prototype using open source Floodlight controller, and evaluate its performance under various DDoS attacks by real hardware testbed based experiments. We aim to propose a practical system built upon SDN to defend against a wide range of flooding-based DDoS attacks, i.e., link flooding (including sophisticated attacks, e.g., Crossfire), SYN flooding, and UDP-based amplification attacks. The proposed system does not need to modify the current packet forwarding diagram and it is compatible with the current IP data plane. We propose RADAR, an architecture aiming to detect various DDoS attacks via adaptive correlation analysis on COTS SDN switches. It does not require any modifications in SDN protocols and switches, nor does it need any extra appliance to detect attacks. RADAR is able to capture and throttle We evaluate the performance by experiments based on a real testbed, and demonstrate that RADAR can effectively and efficiently detect various attacks within short delays.
2. Pham, Thi Ngoc Diep, Chai Kiat Yeo, Naoto Yanai, and Toru Fujiwara."Detecting flooding attack and accommodating burst traffic in delay-tolerant networks." IEEE Transactions on Vehicular Technology 67, no. 1 (2017): 795-808.

   DTN is vulnerable to flooding attack in which malicious nodes flood the network with superfluous data to deplete the network resources. Existing works mitigate internal flooding attacks by rate-limit to constrain the number of messages that nodes can generate per time slot. However, rate-limit cannot flexibly accommodate burst traffic in which nodes may have sending demands higher than the rate-limit for a short period. In this paper, we propose FDER to detect flooding attack and yet allow legitimate burst traffic simultaneously. Nodes exchange their histories of encounter records (ER) which record the sent messages during their previous encounters. The ER history is used to infer a node's new message transmission rate over time and the number of forwarded replicas per message. The adversary nodes that send too many messages or replicas can thus be detected. Since ERs serve as useful tools for monitoring the sending behavior of nodes over a long time period, FDER could detect the burst traffic violation efficiently. Being a serious threat to mobile DTN, flooding attack needs to be tackled to ensure network security. See This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. To balance these two requirements, we propose a framework comprising FDER - a distributed scheme to detect flooding attack and FP - a fairness policy under the context that nodes are allowed to have short burst transmission. Using ER which is an efficient tool to monitor the sending behaviors of nodes for a long period, FDER could differentiate a persistent flooding attack from a burst transmission over a short time.

3. Kohnhäuser, Florian, NiklasBüscher, and Stefan Katzenbeisser."A practical attestation protocol for autonomous embedded systems."In 2019 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 263-278.IEEE, 2019.

   A key technique to guard the secure and safe operation of connected embedded devices is remote attestation. It allows a third party, the verifier, to ensure the integrity of a remote device, the prover. Unfortunately, existing attestation protocols are impractical when applied in autonomous networks of embedded systems due to their limited scalability, performance, robustness, and security guarantees. In this work, we propose PASTA, a novel attestation protocol that is particularly suited for autonomous embedded systems. PASTA is the first that (i) enables many low-end prover devices to attest their integrity towards many potentially untrustworthy low-end verifier devices, (ii) is fully decentralized, thus, able to withstand network disruptions and arbitrary device outages, and (iii) is in addition to software attacks capable of detecting physical attacks in a much more robust way than any existing protocol. We implemented our protocol, conducted measurements, and simulated large networks. . In this work PASTA, a practical attestation protocol for autonomous networks of embedded systems. In PASTA, prover devices periodically collaborate to generate so-called tokens. Each token attests the integrity of all provers that participated in its generation. During token generation, provers mutually ensure their integrity and then make use of a Schnorr-based multisignature scheme to compute an aggregated signature, which is stored in the token and attests the provers' integrity. We showed that PASTA is scalable to very large networks due to its small communication and computational overhead. In the best case, which is a static network with a uniform tree topology and only prover devices, one million provers can attest and verify each others' integrity in less than 2.91 s (token generation and exchange).It provides a scalable and efficient attestation with many provers and many verifiers. In fact, thousands of low-end embedded prover devices are able to attest their integrity in a small token that can be verified by any network device, including low-end embedded and untrustworthy devices. It provides a high level of robustness against device and network disruptions.

4. Seth, Bijeta, SurjeetDalal, VivekJaglan, Dac-Nhuong Le, Senthilkumar Mohan, and GautamSrivastava."Integrating encryption techniques for secure data storage in the cloud." Transactions on Emerging Telecommunications Technologies 33, no. 4 (2022): e4108.

. The economic benefits or rather the fundamental economic shift offered by cloud computing in reducing capital expenditure and converting it to operational expenditure has been a primary motivating factor for early adopters. However, despite its inherent advantages that include better access and control, there exist several reservations around cloud computing that have impeded its growth. The control, elasticity, and ease of use that cloud computing is associated with also engender many security issues. Security is considered to be the topmost hurdle out of the nine identified challenges of cloud computing as underlined by the study conducted by the International Data Corporation. It therefore follows that an exceedingly secure system is essential for the safeguarding of an organizational entity, its resources, and assets. In this article, it is our endeavor to offer insights into the implementation of a novel architecture that can deliver an enhanced degree of security for outsourcing information in a cloud computing environment while involving numerous independent cloud providers. The framework comprises of dual encryption and data fragmentation techniques that envision the secure distribution of information in a multicloud environment. A lot of research activities are ongoing to address cloud security threats.1,2 This article seeks to emphasize the need for effective cloud security countermeasures by discussing various aspects of the cloud security problem. The advantages of using multicloud systems have been described along with the proposed set of four distinct multicloud architectures. Each of these proposed architectures have their distinct pros and cons vis-a-vis the problem of security and these have been represented diagrammatically. Case studies representing real-life examples have also been discussed for each scenario.The architecture includes an overview of algorithms for file slicing and encryption as well as file decryption and merging. A comparison table comparing various existing schemes with the proposed model in terms of turnaround time, encryption process time, security features (privacy, insider attack, secret keys, confidentiality, data integrity, and so on), and reliability features (file formats supported, collusion attack, key escrow, malicious files, file size, and so on) has been listed.

EXISTING SYSTEM

In order to provide data storage employment, cloud storage employs software to interconnect and facilitate collaboration between different types of storage devices. Compared to traditional storage methods, cloud storage poses new challenges in data security, reliability, and governing body. Cloud storage uses application software to make numbers of different types storage devices work jointly and provide assemblage storage and business functions. While we use cloud storage, we need not know the data of the storage devices as we use a several independent storage, which including what model the storage devices are, what the interface and communication protocol are, how many number of disks and what type, how much capacity, what kind of disconnectedness cable between the storage and server was used. User also need not build their corresponding data backup systems and disaster recovery systems to ensure data security and business continuity. In addition, user need not judiciousness about storage equipment condition monitoring, improvement, software and instrumentation updates and upgrades. All the disposition are completely diaphanous to the user in cloud depository system. Any authorized user can connect with cloud storage direct a cable and access data on cloud storage in any place.

Disadvantages

- Does not provide any prior information regarding natural disasters.
- No solution to avoid data loss during disaster.
- Does not provide any encryption for data secure in server.

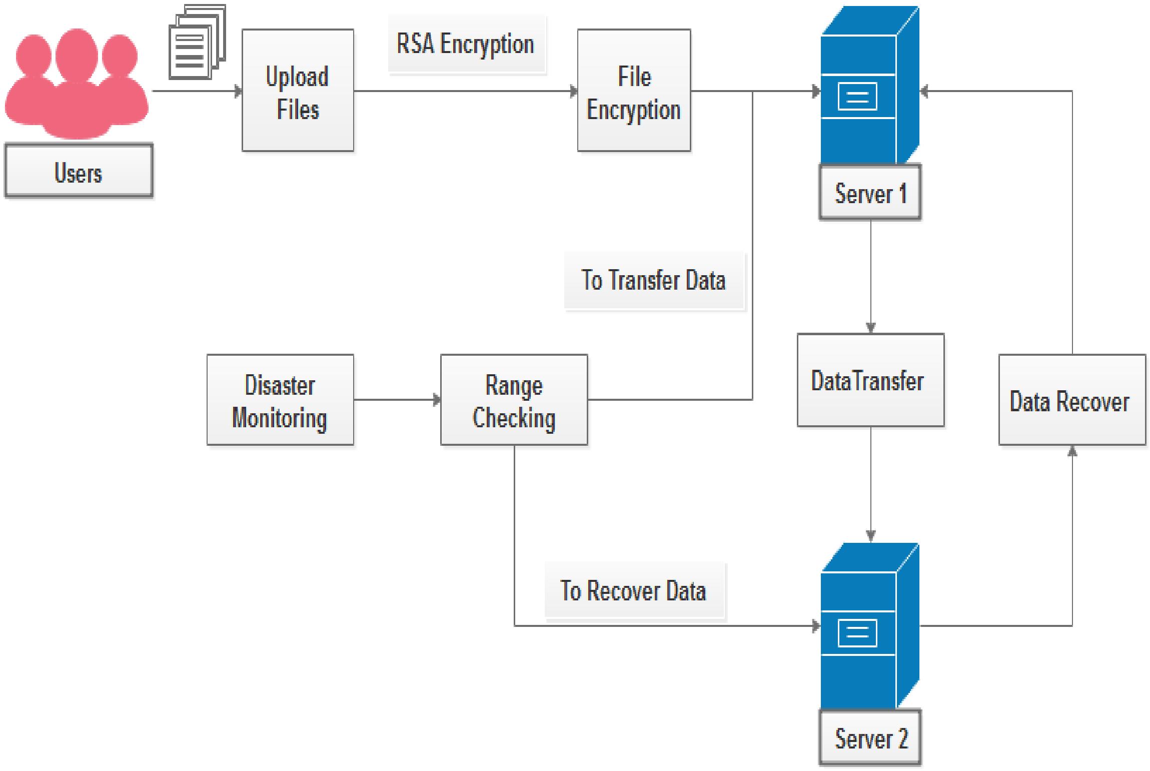
PROPOSED SYSTEM

In order to provide data keeping services, atmospheric phenomenon storage employs software to interconnect and facilitate collaboration between different variety of depository devices. Compared to long-standing storage methods, cloud storage poses new inquiring in data security, responsibleness, and management. Physical phenomenon storage uses application package to make numbers of contrasting types storage devices work put together and provide data storage and business scientific discipline relation. The optimum disaster recovery preparation should take into thought process the fundamental parametric quantity including the initial cost, the cost of data transfers, and the cost of data storage. The organization data needs and its bad luck advance objectives need to be considered. To evaluate the risk, the variety of hard knocks (natural or human-caused) need to be known. The chance of a disaster sensual event needs to be assessed on with the costs of comparable to success. An grade-appropriate approach for the value judgement needs to be bolshy to allow a one-twelfth assessment of shortly active disaster convalescence plans (DRP) in terms of the time period need to restore the assist (associated with RTO) and affirmable red ink of data (associated with RPO).

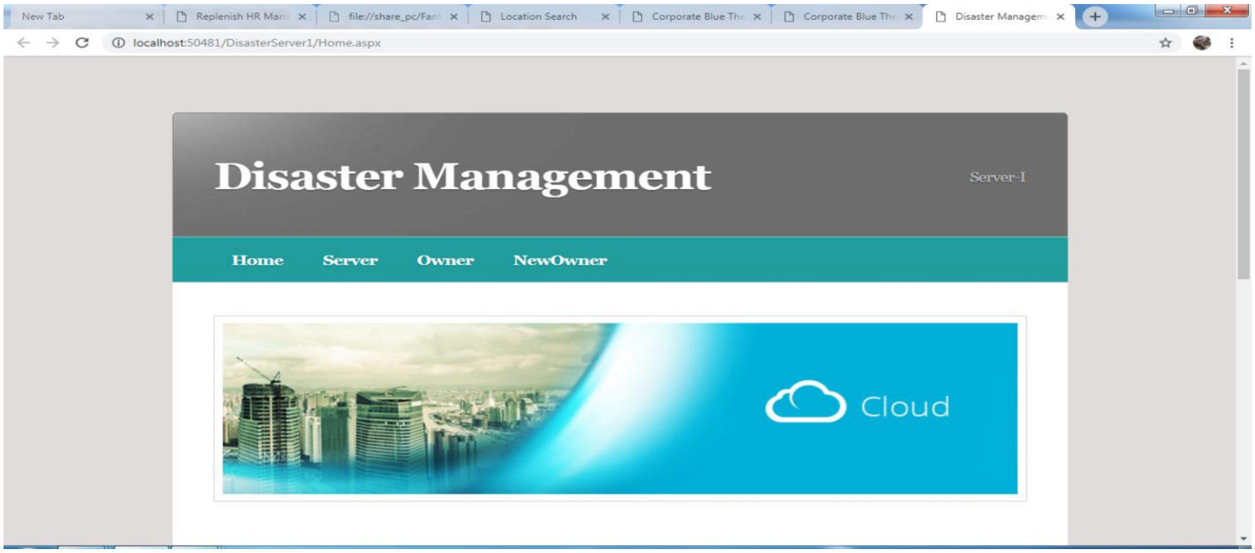
Advantages

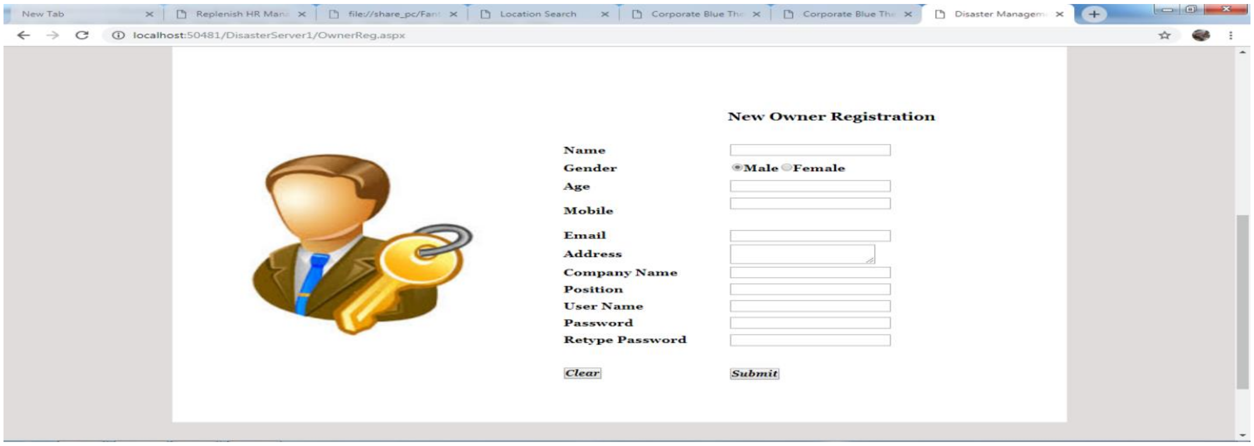
- To provide efficient disaster recovery approach before the data loss.
- RSA based secure encryption mechanism is implement for data encryption.
- Data recovery process is also ensures the efficient retrieval of data.
- To control the risk of data loss, it is required to monitor the recovery point.

PROPOSED SYSTEM ARCHITECTURE



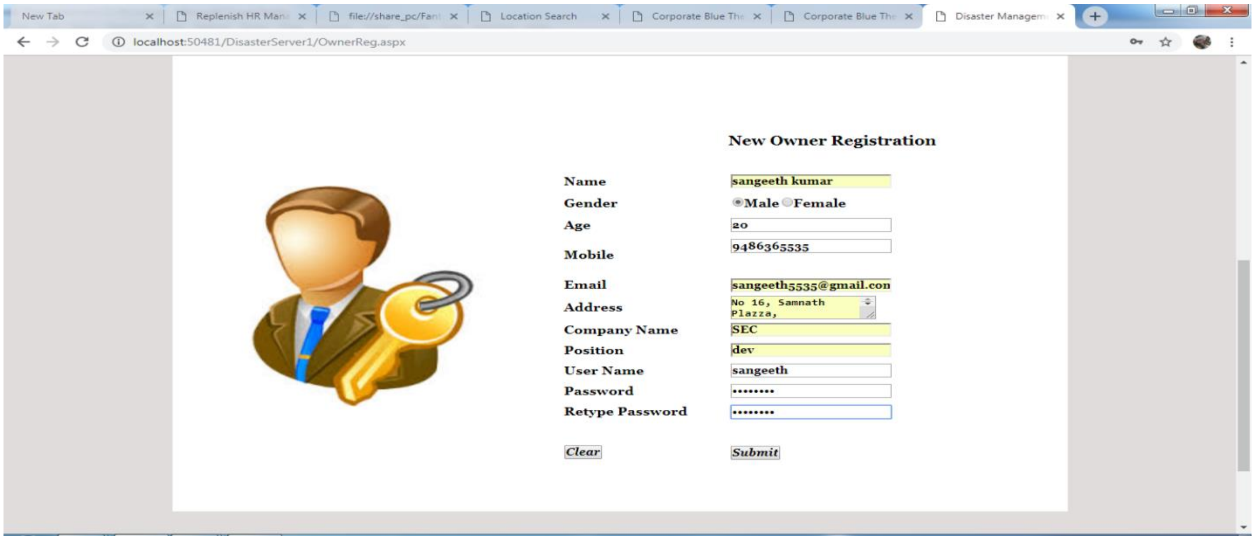
IMPLEMENTTION:





New Owner Registration

Name	
Gender	● Male ○ Female
Age	
Mobile	
Email	
Address	
Company Name	
Position	
User Name	
Password	
Retype Password	
Clear	Submit



New Owner Registration

Name	sangeeth kumar
Gender	● Male ○ Female
Age	20
Mobile	9486365535
Email	sangeeth5535@gmail.con
Address	No 16, Samnath Plazza,
Company Name	SEC
Position	dev
User Name	sangeeth
Password	••••••••
Retype Password	••••••••
Clear	Submit

CONCLUSION

As cloud computing is becoming very important in day to day life and every establishment is based on cloud computing. They are not alert of disasters in cloud; they don't know any deed action at first. When tough circumstances occurred then all organisation faced astronomical loss of data and also business then after many another recovery mechanisms are acquaint. As cloud language has a PaaS, IaaS, and SaaS as services which ply their service to feeling users in damage of store, software and papers as their requirement; so user can use cloud without any disturbance. By apply DRaaS in cloud one can get recovered from collection loss when he experiences a system occurrent or by natural flower. Tonic solfa syllable by use DRaaS in enterprise lastingness they can get the better of their data loss.

FUTURE ENHANCEMENT

Our ongoing lookup is unfocused on promote high engineering science and elimination of the erring tasks of hard knocks recovery thinking, asseveration back, lengthways activity optimization, deposit service rootage, and others that are before long dead using back-of-the-envelope computing. Establishment judgment are unobjectionable much old-fashioned military installation facto kinda than being reactive.

REFERENCES

[1] Zheng, Jing, Qi Li, GuofeiGu, Jiahao Cao, David KY Yau, and Jianping Wu. "RealtimeDDoSdefense using COTS SDN switches via adaptive correlation analysis." IEEE Transactions on Information Forensics and Safety 13, no. 7 (2018): 1838-1853.

[2] Pham, Thi Ngoc Diep, Chai Kiat Yeo, Naoto Yanai, and Toru Fujiwara."Detecting flooding attack and kind burst traffic in delay-tolerant networks." IEEE Proceedings on Vehicular Technology 67, no. 1 (2017): 795-808.

[3] Kohnhäuser, Florian, NiklasBüscher, and Stefan Katzenbeisser."A practical attestation protocol for autonomous embedded systems."In 2019 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 263-278.IEEE, 2019.

[4] Seth, Bijeta, SurjeetDalal, VivekJaglan, Dac-Nhuong Le, Senthilkumar Mohan, and GautamSrivastava."Integrating encryption techniques for secure data storage in the cloud." Transactions on Emerging Telecommunications Technologies 33, no. 4 (2022): e4108.

[5] Chen, Min, Wei Li, Giancarlo Fortino, YixueHao, Long Hu, and IztokHumar."A dynamic service migration mechanism in edge cognitive computing." ACM Transactions on Internet Technology (TOIT) 19, no. 2 (2019): 1-15.