Submitted by: Sajan Maharjan

POVIS ID: thesajan@postech.ac.kr

CSED 601 Take-home Mid-term 2018/Fall semesterDue: 10/23(Tue.) 13:00 ~ 18:00This is an open-book, open-note, and take-home exam. You will be graded based on  
the depth of investigation and logical organization of your answer. You have to list all  
materials you have referenced. All works should be an individual work without any help  
from others.

*1. (15 pts) According to the definition of “cloud computing” in Wiki, it refers  
“hardware machine or group of computing hardware machines commonly referred  
as a server connected through a communication network such as internet , intranet,  
local area network (LAN) or Wide area network (WAN) and individual user or  
users who have permission to access the server can use the server's processing  
power for their individual computing needs like to run an application, store data or  
any other computing needs alike.” It has three service models known as “IaaS”,  
“PaaS”, and “SaaS”. It is commonly believed that the more modules you have, the  
more problems you will get. To provide a reliable service to users, what  
techniques are needed in Cloud computing? Your answers should be described in  
terms of redundant resources and techniques of using redundant resources.*

Answer> The following techniques can be used for obtaining reliable services in cloud computing-

* Checking and Monitoring- The system is constantly monitored at runtime to validate, verify and ensure that correct system specifications are being met. This technique, while simple, plays a key role in failure detection and subsequent reconfiguration
* Checkpoint and Restart- The system state is captured and saved based on pre-defined parameters (e.g., after every 1024 instructions or every 60 seconds). When the system undergoes a failure, it is restored to the previously known correct state using the latest checkpoint information (instead of restarting the system from start).
* Replication- Critical system components can be duplicated using additional hardware, software and network resources in such a way that the critical components is available even after the failure happens. This method can be used to prevent failures of the hard disk or a server failure by switching from a failed primary system to a backup system. Replicas can be maintained in ***hot standby*** mode. For example, redundant capacity is configured in three cloud regions to provide stable cloud service through redundant connection because the same data exists in the remaining two cloud regions even if a failure occurs in one cloud region. As a practical example, Amazon uses ‘zero virtual replication’ based on CDP (Continuous Data Protection) to replicate changes in real time, and Microsoft's Azure uses ZRS (local redundant storage) zone redundant storage, and geo-redundant storage (GRS) to store and locate redundant resources from the local to the local area.

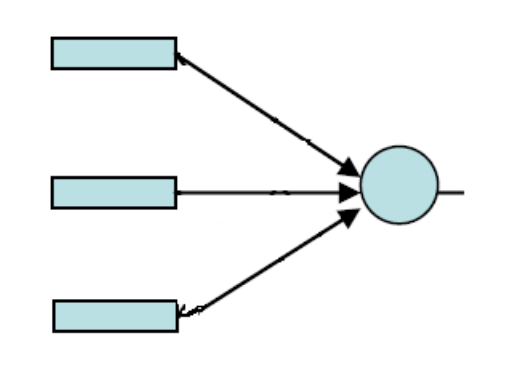
*2. (15 pts) A blockchain, originally block chain, is a growing list of records, called* blocks, *which are linked using cryptography. Each block contains a cryptographic hash of the  
previous block, a timestamp, and transaction data (generally represented as a merkle  
tree root hash). For use as a distributed ledger, a blockchain is typically managed by  
a peer-to-peer network collectively adhering to a protocol for inter-node communication  
and validating new blocks. Once recorded, the data in any given block cannot be altered  
retroactively without alteration of all subsequent blocks, which requires consensus of the  
network majority. Describe what redundancy techniques are used to make the  
distributed ledger a dependable technique.*

Answer> The blockchain is a distributed ledger maintained by a peer to peer network in which records are grouped into blocks and added in the open-distributed ledger secured by a cryptographic hash such that each block is sequentially linked with the previous block. Records inserted into the blockchain are immutable and secure from tampering. Such dependability in the blockchain is achieved through the following redundancy techniques-

* Information Redundancy- Blockchain is maintained in a decentralized, distributed manner. This means that there is no central authority or a single point of failure in the system. Each full node maintains the latest updated copy of records/transactions in the blockchain. This can be understood as a duplication of the same data over the entire distributed network. And so, even if a single node in the system fails, the same information is present in the rest of the nodes, due to which the system can still function its operations. In this way, redundant copy of ***data/information*** over nodes protect the blockchain from failure.
* Time Redundancy- Time redundancy is the technique by which systems attempts to be fault tolerant by expending additional time by executing instructions. Cryptography is an example of time redundancy technique whereby the change in the volume of data is incomparable to the time spent while encrypting or decrypting data. Similarly, in blockchain, each block is hashed using unidirectional hashing algorithm i.e. SHA-256 and addresses and keys are also generated using public key cryptography. Also in the case of mining blocks in the blockchain, miners spent significant time trying to find the nonce value solution, in which the block hash (generated using merkle root, timestamp, difficulty, nonce value) should be less than a specific bit values and the only way to do so is to repeatedly try generating the blockhash by incrementing the nonce value.

Others techniques that are employed to make the blockchain secure are- consensus protocols algorithms and mining rewards. In a distributed system, where there is no central authority, different nodes will have different copies/versions/opinions of data. Specifically in blockchain, there is a notion of the Double Spending Problem, whereby a single coin is spent twice by a malicious node. In order to prevent double spending, each node will have to establish a baseline truth among other nodes which is done using a consensus algorithm such as Proof Of Work, Proof Of Stake, Delegated Proof of Stake, etc. Blockchain also incentivizes miners with mining rewards for acting honest which also makes the blockchain secure and dependable.

*3. Answer to the following questions.  
A. (3 pts) Find the reliability of a TMR, which is shown in the below left side,  
using combinatorial approach. Individual module’s reliability is Rm and  
voter’s reliability is Rv.*



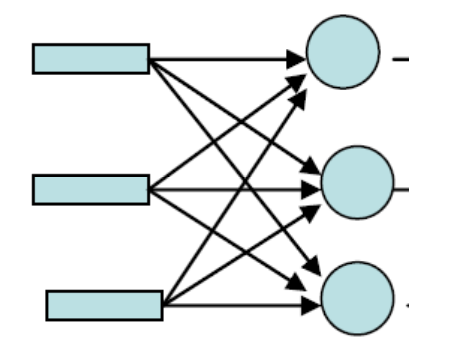
Answer> The module in TMR can be thought of as a 2 of 3 model in parallel whose reliability is given as-

Rm(2 of 3) = Rm3 + C(3,2)Rm2(1-Rm)*c* = 3Rm2 – 2Rm3 (Assumingcoverage *c* is 1)

This module is in series with the voter, thus the reliability of the TMR system is-

RTMR = Rv(3Rm2 – 2Rm3)

*B. (4 pts) Find the reliability of a TMR with triplicated voters, which is shown  
in the above right side, using combinatorial approach. Individual module’s  
reliability is Rm and voter’s reliability is Rv.*



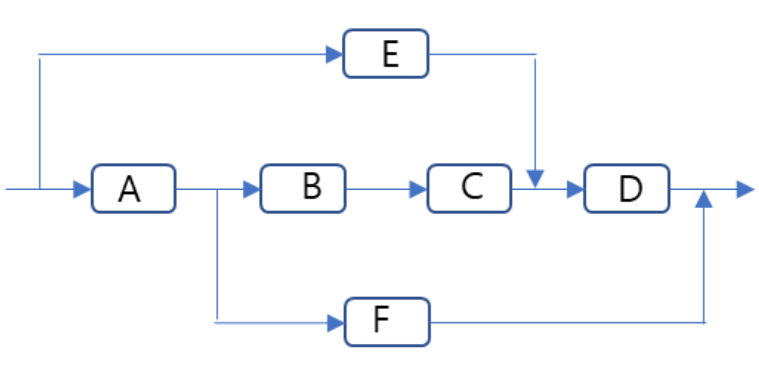
The above shown triplicated voter can be thought of as 3 TMRs arranged in parallel. So the reliability of the above system is-

RtriplicatedTMR = (1 – (1 – RTMR)3)

where RTMR = Rv(3Rm2 – 2Rm3)

*C. (4 pts) Find the reliability of a modified restoring organ which is shown in  
the below using combinatorial approach. Individual module’s reliability is  
R(i)m and voter’s reliability is R(i)v  
D. (4 pts) Find the reliability of an original restoring organ which is shown in  
the below using combinatorial approach. Individual module’s reliability is  
R(i)m and voter’s reliability is R(i)v*

*4. (10 pts) Find the reliability of the following system using non-series/non-parallel  
combinatorial approach.*



* Assuming the node D fails, there is only a single path to the system.The reliability of the sub system becomes- (1-RD)RA.RF
* When node D is operational with reliability RD , we can think of the paths- E, ABC or AF
  + When node E fails, we can think of the path- ABC or AF, then the reliability of the sub system is-

((1 - (1-RBRC).(1 – RF)))(1 - RE)

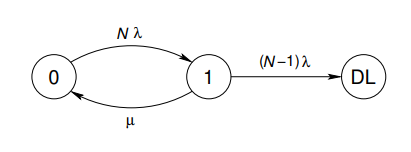
* When node is operational with reliability RE, the subsystem will have reliability of RE.1

Therefore, the reliability of the system can be obtained by adding the component reliabilities as-

Rsys = RD(((1 - (1-RBRC).(1 – RF)))(1 - RE) + RE) + (1-RD)RA.RF

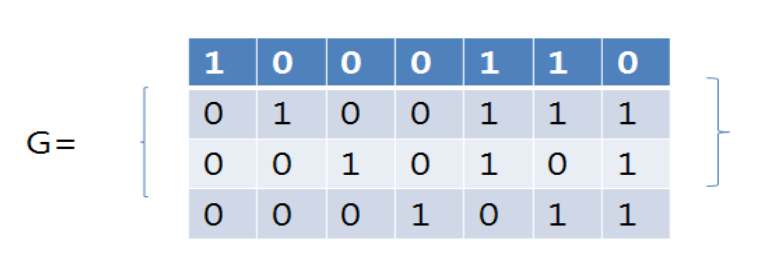
*5. (10 pts) Assume that there is a RAID system with 4 disks. Also assume that each  
disk has a same failure rate. The RAID system has taken RAID 5 configuration –  
rotating parity block . Draw a Markov chain to analyze the reliability of this  
RAID system. You need to show a transition rate between states. Also you have to  
specify what state(s) is(are) corresponding to failure state. Assume that the RAID  
system is considered failed if there exists a block that cannot be recovered due to  
disk failures.*

Answer>



Replacing N with 5 gives us the appropriate markov chain diagram

*6. Answer to the following questions  
A. (6 pts) The following parity check generation matrix for (7,4)-parity code  
has a capability of detecting a single bit error with position. Find a matrix H  
that is used to check non-error or the position of a faulty bit.*



Answer> We know that the generator matrix can be represented as-

G = [ I | P ]

where I = identity matrix of 4X4 = [[ 1 0 0 0 ]

[ 0 1 0 0 ]

[ 0 0 1 0 ]

[ 0 0 0 1 ]]

and P = parity matrix = [[ 1 1 0 ]

[ 1 1 1 ]

[ 1 0 1 ]

[ 0 1 1 ]]

then the H matrix can be obtained using the formula- H = [ PT | I ]

where PT = transpose of P = [[ 1 1 1 0 ]

[ 1 1 0 1 ]

[ 0 1 1 1 ]]

And I is a 3 X 3 identity matrix

Therefore, H = [ PT | I ] = [[ 1 1 1 0 1 0 0]

[ 1 1 0 1 0 1 0]

[ 0 1 1 1 0 0 1]]

*B. (4 pts) Explain or prove that the code system above has not a capability of  
detecting a double-bit error.*

In hamming codes, the parity bits occupy the positions 1, 2 and 4 (power of 2). The remaining are data positions-

1 2 3 4 5 6 7

c1 c2 d1 c3 d2 d3 d4

The value of the parity bits can be obtained by the relations-

c1 = d1 XOR d3 XOR d4

c2 = d2 XOR d3 XOR d4

c3 = d1 XOR d2 XOR d3

This hamming code is capable of detecting and correcting single errors. By adding another parity bit, which contains the parity of the Hamming code word, one can obtain a code with a Hamming distance of 4. Such codes can detect double bit errors and correct single errors.

*7. Answer to the following questions. (IoT Security & Dependability)  
A. (5 pts) In IoT environments, sensors and actuators are important for correct  
operation. Suggest schemes to enhance the dependability of sensory inputs  
and actuator control outputs.*

*B. (10 pts) In blockchain, it uses a Merkle-tree to get an integrity check of all  
transactions included in a block. From the viewpoint of designing a  
dependable block, what dependability aspects are supported by Merkle tree  
and what are missing. If it provides some dependability aspects, discuss  
what redundancy schemes are used to get such dependability aspects.*

Answer> A Merkle root is the hash of all the hashes of all the transactions that are part of a block in blockchain. A merkle tree root hash ensures that all the transactions contained in the block are defined by the hash value of the merkle root. The transaction hash of all the transactions in the block are hashed with one another in an iterative bottom up approach to generate a single hash of length 256 bits called the merkle root. Using a Merkle root approach provides the following dependability aspect-

Security- Both integrity and confidentiality is preserved by the use of merkle root in the blockchain. In case a malicious attacker wants to modify a single transaction hash, he/she will have to modify all the transactions included in that block since they follow a bottom up approach. This makes the tampering of merkle root or transactions difficult. Hashing algorithms maintain the confidentiality in the block.

Availability- Availability in the sense that the merkle root when generated is formed by iterative hashing of each transactions in the block. If the value of merkle root matches with the hash generated by hashing each individual transaction, we can assume that all transactions are available in that block.

Reliability- By ensuring that the merkle root hash value is the correct value, reliability is achieved.

Safety and Maintainability aspects are not applicable to the merkle root hash generation. The above mentioned security, availability and reliability aspects are achieved through the following redundancy schemes-

Information Redundancy- Double-Hashing of SHA-256 algorithms is used to generate the merkle root hash.

Time Redundancy- A block can contain varying number of transactions, so that the number of times the double hashing will take place is not fixed. In the end, irrespective of the number of transactions in the block, a fixed length merkle root of 256 bits is generated, by repeating the hashing process time and again.

*8. Security attack is considered as an attempt to generate a fault by a human  
intentionally. Answer to the following questions.  
A. (3 pts) Suggest one hardware redundancy approach to block security attacks.*

Answer> Self Purging Redundancy such that faulty modules are moved out of operations themselves

*B. (3 pts) Suggest one software redundancy approach to block security attacks.*

Answer> Algorithm Construction. Eg. Consensus algorithms such as Proof of Work, Proof of Stake are used in blockchain to prevent double spending attack

*C. (4 pts) Describe what would be a good measure to evaluate the security prevention ability of a system.*

Answer>Risk can be used as a quantitative measure of security.

**References Used:**

<https://www.investopedia.com/terms/m/merkle-root-cryptocurrency.asp>

<https://people.kth.se/~dubrova/FTCcourse/LECTURES/lecture6.pdf>

<https://blockgeeks.com/guides/what-is-blockchain-technology/>

<https://air.unimi.it/retrieve/handle/2434/233330/304980/phd_unimi_r09220.pdf>

Fault Tolerance in Distributed Systems, Jalote