International Journal of Mathematical, Engineering and Management Sciences
Vol. 6, No. 1, 15-29, 2021
https://doi.org/10.33889/IJMEMS.2021.6.1.003

Survivability and Vulnerability Analysis of Cloud RAID Systems under Disk Faults and Attacks

Qisi Liu
Department of Electrical and Computer Engineering,
University of Massachusetts, Dartmouth, MA, USA.
E-mail: qliu1@umassd.edu

Liudong Xing
Department of Electrical and Computer Engineering,
University of Massachusetts, Dartmouth, MA, USA.
Corresponding author: lxing@umassd.edu

(Received May 14, 2020; Accepted July 1, 2020)

Abstract
In this paper we model and analyze survivability and vulnerability of a cloud RAID (Redundant Array of Independent Disks) storage system subject to disk faults and cyber-attacks. The cloud RAID survivability is concerned with the system's ability to function correctly even under the circumstance of hazardous behaviors including disk failures and malicious attacks. The cloud RAID invulnerability is concerned with the system's ability to function correctly while occupying some state immune to malicious attacks. A continuous-time Markov chains-based method is suggested to perform the disk level survivability and invulnerability analysis. Combinatorial methods are then presented for the cloud RAID system level analysis, which can accommodate both homogeneous (based on binomial coefficients) and heterogeneous (based on multi-valued decision diagrams) disks. A detailed case study on a cloud RAID 5 system is conducted to illustrate the application of the proposed methods. Impacts of different parameters on the disk and system survivability and invulnerability are also investigated through numerical analysis.

Keywords- Cloud storage system, Cyberattack, Disk fault, Survivability, Vulnerability.

1. Introduction

Survivability is concerned with the ability of a system to continue its intended operation in the presence of accidental failures or malicious attacks (Fung et al., 2005). Going beyond the survivability, the invulnerability of a system is concerned with the system's ability to function correctly while occupying certain state immune to malicious attacks. In addition to the individual component failures caused by factors like aging and defects, various cyber-attacks have posed significant threats to modern technological systems such as Internet of Things, cloud computing systems (Chou, 2013; Escudero et al., 2018; George and Thampi, 2018; Xing, 2020). For instance, sound waves have been utilized to launch DoS (denial-of-service) attacks without internet connections, causing the service outage even hardware damages (e.g., destroying electronic devices, or posing a life-threatening danger on medical devices) (Shahrad et al., 2018). The objective of this paper is to quantitively assess the survivability and invulnerability of a cloud RAID (Redundant Array of Independent Disks) storage system at both disk and system levels, facilitating the robust design and operation of the cloud RAID system in practice.

Reliability analysis of cloud storage systems has received significant attentions from both academia and industries, which focused only on the system behavior in the event of random component failures, see for example, Iliadis et al. (2014), Liu and Xing (2015a, 2015b), Mandava and Xing

(2019, 2020), Nachiappan et al. (2017), and Zhang et al. (2013). In contrast to the rich literature for quantitative reliability analysis, there exist only limited works on quantitative security analysis, see for example, Levitin et al. (2018), Liu et al. (2019), and Xu et al. (2019). This paper advances the state of the art by performing survivability and vulnerability modeling and analysis of cloud storage systems, simultaneously considering both reliability and security attributes. We analyze possible threat scenarios through a survivability architecture. We then examine the failure and attack behaviors at the disk level and propose a continuous-time Markov chains (CTMC)-based method to assess the survivability and invulnerability of each disk in the cloud RAID system. Based on the disk level analysis, we then present combinatorial methods to quantify the survivability and invulnerability of the entire cloud storage system.

The rest of the paper is structured as follows. Section 2 presents the framework or architecture of survivability modeling. Section 3 presents an illustrative example of a cloud RAID storage system. Section 4 presents the CTMC-based method and the combinatorial methods. Section 5 presents detailed analyses of the example cloud RAID system at the disk level and investigates impacts of several attack or recovery parameters on the disk performance. Section 6 performs the system level survivability and invulnerability analysis. Lastly, Section 7 gives conclusions and identifies directions for future work.

2. Survivability Architecture

Figure 1 depicts a three-level survivability architecture. At the bottom level, representative hazardous events are listed. In particular, according to the cloud vulnerability incidents investigation report (Check Point, 2020; Ko et al., 2013), the top three threats to the CIA (confidentiality, integrity, availability) were Insecure Interfaces & APIs (29% of all threats), Data Loss & Leakage (25%), and Hardware Failure (10%). These three threats accounted for 64% of all the cloud outages investigated in the report. Specifically, APIs are the inter-connector which provide the interface between the Internet and the Things. Since the APIs are accessible from anywhere on the Internet, malicious attackers can use them to compromise the confidentiality and integrity of the system or service (attackers acquiring a token employed by a customer to get access to the service via the service API can make use of the same token to manipulate this customer's data) (Bamiah and Brohi, 2011). Regarding the Data Loss & Leakage threat, an attacker might steal, modify or corrupt the data, for example through the co-resident or co-location attacks (Hasan and Rahman, 2020; Xing et al., 2019). In addition, this work also addresses another common form of cyberattacks, the distributed DoS (DDoS) attacks, which are designed to take over all network, storage and server resources with transient bursts, causing cloud services to crash (Wang et al., 2015). The frequency of DDoS attacks has increased more than 2.5 times over the last 3 years. The average size of DDoS attacks has correspondingly grown approaching 1 Gbps, which is enough to take most organizations completely offline (Avital et al., 2020; Hummel, 2019). There exist other threats that are not addressed in this work, such as Account/Service Hijacking, Abuse and Nefarious Use of Cloud, Malicious Insiders, and etc. (Bamiah and Brohi, 2011).

The bottom level also covers representative causes for generating hardware, software or middleware faults, including implementation mistakes, external disturbances, and component flaws or defects. In the middle level, the effects from the hazardous causes are identified, including the effects to the CIA principle of vulnerabilities and the three types of faults. Techniques or mechanisms can be developed to mitigate or tolerant these faults, enhancing the system survivability. For example, security controls (e.g. correct firewall setting and certain windows updates) could reduce the security risk effectively. Redundant techniques (e.g., standby sparing, *N*-

International Journal of Mathematical, Engineering and Management Sciences
Vol. 6, No. 1, 15-29, 2021
https://doi.org/10.33889/IJMEMS.2021.6.1.003

modular redundancy) can be implemented to achieve fault tolerance. However, due to the imperfectness of these mitigation strategies and complicated interdependencies among the system components, the system may still fail leading to the loss of the system assets or the mission despite the use of the survivability enhancement techniques.

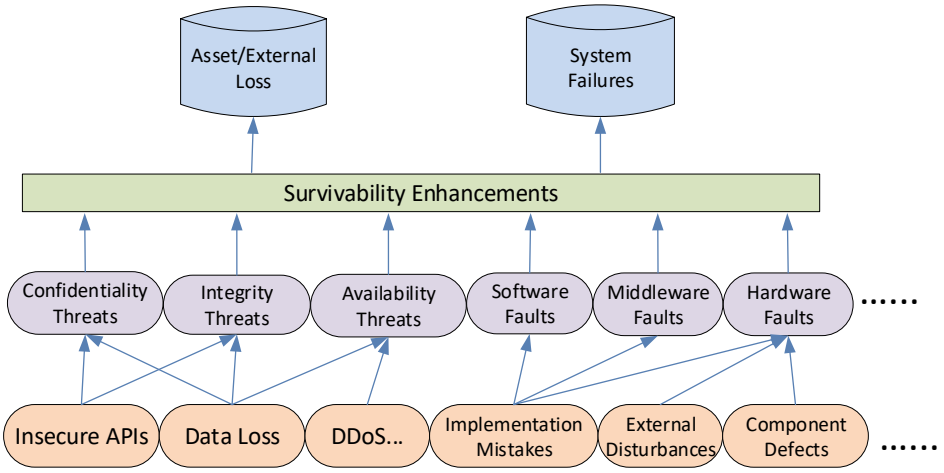

Figure 1. Survivability architecture.

3. Example Cloud RAID System Description

The cloud RAID 5 with four disks in the array is used as an illustrative example system (Liu and Xing, 2015b). As shown in Figure 2, data are divided into stripes or blocks and are stored across four different disks that may be from different providers). The parity information (Ap, Bp, Cp, Dp) is also distributed among the four disks, providing fault tolerance in the event of one disk failure or being attacked. More specifically, when one disk malfunctions, the system can restore the stripes of the failed disk using the parity stripe and remaining data stripes easily, for example through the exclusive OR operation.

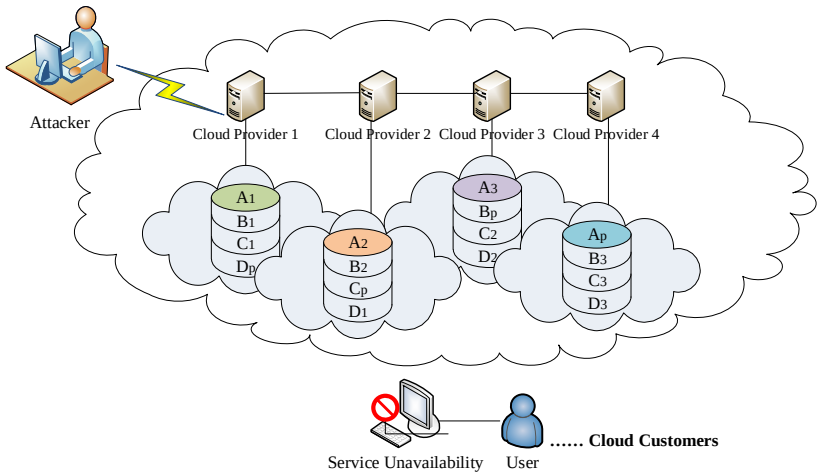

Figure 2. An example cloud RAID 5 system.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 6, No. 1, 15-29, 2021
https://doi.org/10.33889/IJMEMS.2021.6.1.003

4. Proposed Method

The proposed method includes a CTMC-based model for describing the complicated failure, attack and recovery behaviors of an individual disk and further evaluating the state probabilities at the disk level. The method also covers a multi-valued decision diagram (MDD)-based combinatorial model for the system level survivability and invulnerability analysis.

4.1 CTMC-Based Disk-Level Solution

Figure 3 illustrates the CTMC model, i.e., the state transition diagram depicting the attack, failure and recovery behaviors of a RAID disk. In the initial good state 0, the disk possesses both the security and reliability attributes (the data can be retrieved from the disk correctly). From the good state, the disk can transit to the degradation state 1 with rate λ_{gd}. It may then transit back to the good state with rate μ_{dg} due to the disk's self-recovery mechanism that is able to restore certain media errors. In the event of the restoration attempt failing, the data get permanently lost and the disk transits to the failure state 3 with rate λ_{df}. From the initial good state, due to DDoS attacks or even events that bring transiently explosive server visits (e.g., Black Friday online shopping), the disk drive may enter the vulnerable state 2 with rate ρ_{gv}; under this state some latency problems occur but the system still works. The disk can go back to the good state 0 from the vulnerable state 2 with performing contingency strategies immediately with recovery rate r_{vg}. However, under the state 2, if no timely remedial measures are taken or the size of the attacks increases, the disk server can go down anytime entering the failure state 3 with rate ρ_{vf}. The inaccessibility of a disk in the failure state 3 caused by the occurrence of DDoS attacks can be restored fully with rate r_{fg} (back to the good state 0) through some defensive mechanism (e.g., buying enough spare bandwidth for volumetric attacks, developing an incident response plan, haring a DDoS mitigation service) (Mirkovic and Reiher, 2004). The disk can also transit directly from the initial good state 0 to the failure state 3 with rate λ_{gf} due to hardware failure or some unrecoverable failure or with rate ρ_{gf} due to security threats like data tempering/deletion via insecure APIs.

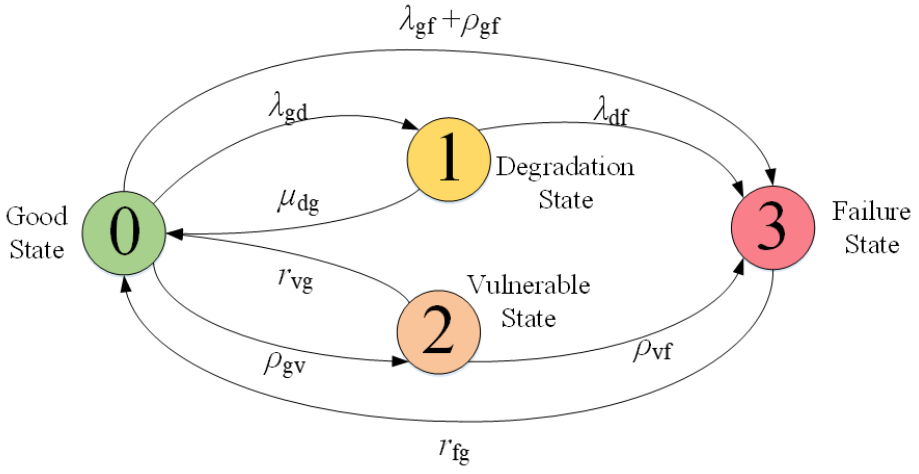

Figure 3. CTMC model of a single RAID disk subject to faults and attacks.

With the state transition diagram (Figure 3), we give the state equations of the CTMC in Eq. (1). Since there are four states, the transition rate matrix in Eq. (1) is a four by four matrix containing all the possible transition rates with the diagonal elements being the negative of the sum of all the

International Journal of Mathematical, Engineering and Management Sciences
Vol. 6, No. 1, 15-29, 2021
https://doi.org/10.33889/IJMEMS.2021.6.1.003

rates on the same column. $P_j(t)$ in Eq. (1) denotes the probability that the disk is in state j (j=0,1,2,3), and $\dot{P}_j(t)$ denotes the derivative of $P_j(t)$ with respect to t. From Eq. (1), Eqs. (2)-(5) can be derived.

$$\begin{bmatrix} -(\lambda_{gd}+\rho_{gv}+\lambda_{gf}+\rho_{gf}) & \mu_{dg} & r_{vg} & r_{fg} \\ \lambda_{gd} & -(\mu_{dg}+\lambda_{df}) & 0 & 0 \\ \rho_{gv} & 0 & -(r_{vg}+\rho_{vf}) & 0 \\ \lambda_{gf}+\rho_{gf} & \lambda_{df} & \rho_{vf} & -r_{fg} \end{bmatrix} \begin{bmatrix} P_0(t) \\ P_1(t) \\ P_2(t) \\ P_3(t) \end{bmatrix} = \begin{bmatrix} \dot{P}_0(t) \\ \dot{P}_1(t) \\ \dot{P}_2(t) \\ \dot{P}_3(t) \end{bmatrix} \quad (1)$$

$$\dot{P}_0(t) = -(\lambda_{gd}+\rho_{gv}+\lambda_{gf}+\rho_{gf})P_0(t) + \mu_{dg}P_1(t) + r_{vg}P_2(t) + r_{fg}P_3(t), \quad (2)$$

$$\dot{P}_1(t) = \lambda_{gd}P_0(t) - (\mu_{dg}+\lambda_{df})P_1(t), \quad (3)$$

$$\dot{P}_2(t) = \rho_{gv}P_0(t) - (r_{vg}+\rho_{vf})P_2(t), \quad (4)$$

$$\dot{P}_3(t) = (\lambda_{gf}+\rho_{gf})P_0(t) + \lambda_{df}P_1(t) + \rho_{vf}P_2(t) - r_{fg}P_3(t). \quad (5)$$

Applying the Laplace transform-based method to solve Eqs. (2)-(5) (using the initial state probability $P_0(0)=1$) and the sum of all the four state probabilities being 1 (Widder, 2015), we obtain the Laplace transform of those state probabilities as:

$$P_1^*(s) = (1+\frac{r_{fg}}{s})/[\frac{a(\lambda_{gf}+\rho_{gf})}{\lambda_{gd}} + \frac{a\rho_{gv}\rho_{vf}\lambda_{gf}}{b\lambda_{gd}} + (s+r_{fg})(\frac{a}{\lambda_{gd}}+1+\frac{a\rho_{gv}}{b\lambda_{gd}})], \quad (6)$$

Where, $a=\mu_{dg}+\lambda_{df}+s$, $b=r_{vg}+\rho_{vf}+s$;

$$P_2^*(s) = \frac{a}{\lambda_{gd}}P_1^*(s), \quad (7)$$

$$P_3^*(s) = \frac{a\,\rho_{gv}}{b\lambda_{gd}}P_1^*(s), \quad (8)$$

$$P_0^*(s) = \frac{1}{s} - P_1^*(s) - P_2^*(s) - P_3^*(s). \quad (9)$$

Applying the inverse Laplace transform of $P_j^*(s)$ (j=0,1,2,3) in Eqs. (6)-(9), the disk state probabilities in the time domain $P_j(t)$ (j=0,1,2,3) can be derived, which is carried out by Matlab in this work.

4.2 Combinatorial System-Level Solution

In order to calculate the system survivability and invulnerability, each disk is modeled as a multi-state component, and the MDD model is applied to represent system-level behavior of the cloud RAID system (Xing and Amari, 2015; Xing and Dai, 2009). Specifically, as illustrated in Figure 4 each multi-state disk k (k=1,2,3,4) is modeled as a non-sink node with four outgoing edges, representing the disk being in the good (0), degradation (1), vulnerable (2), and failure (3) states, respectively. Each edge is associated with its corresponding state probability, denoted by P_{k0}, P_{k1}, P_{k2}, P_{k3}, respectively.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 6, No. 1, 15-29, 2021
https://doi.org/10.33889/IJMEMS.2021.6.1.003

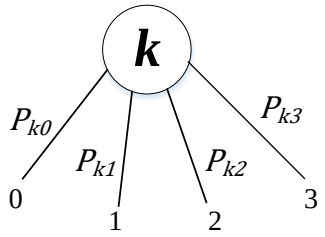

Figure 4. An MDD non-sink node modeling disk *k*.

The entire cloud-RAID 5 system also has four states: good, degraded, vulnerable and failed. Specifically, the entire cloud-RAID system is considered being in a failed state when at least 2 disks are in the failure state 3, modeled using the 2-out-of-4 MDD lattice structure in Figure 5. Sink node 1 in Figure 5 means the system is in the failed state; sink node 0 means the system is not in the failed state. The probability of the system being at the failed state $P_{sys=3}(t)$ is obtained as the sum of probabilities of all the paths from the root node 1 to sink node '1', which is given by Eq. (10).

$$P_{sys=3}(t) = P_{13}P_{23}+(1-P_{13})P_{23}P_{33}+(1-P_{13})(1-P_{23})P_{33}P_{43}+ P_{13}\,(1-P_{23})\,P_{33} \\ +(1-P_{13})\,P_{23}\,(1-P_{33})\,P_{43}+ P_{13}\,(1-P_{23})(1-P_{33})\,P_{43}, \quad (10)$$

where, P_{kj} is the probability of disk *k* being in state *j* (*k* =1, 2, 3, 4, and *j*=0, 1, 2, 3).

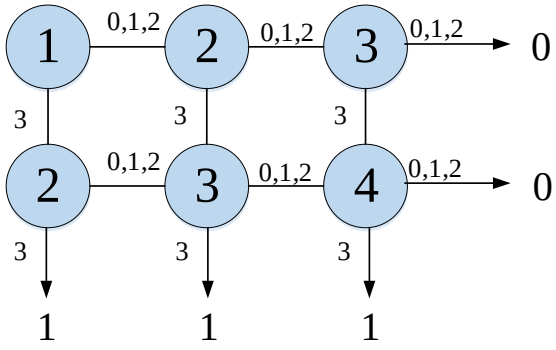

Figure 5. MDD for the cloud RAID 5 in the failed state.

In the case of all the four disks being identical (i.e., having the same state probabilities $P_{kj}= P_j$), the system failed state probability can be simply obtained using binomial coefficients as Eq. (11).

$$P_{sys=3}(t) = C_4^2(P_3)^2\,(1- P_3)^2 + C_4^3(P_3)^3(1-P_3) + C_4^4(P_3)^4. \quad (11)$$

The entire cloud-RAID system is considered being in a good state 0 when at least three out of the four disks are in the good state. The entire system is in the vulnerable state when at least two of the four disks are in the vulnerable state and no two disks are in the failure state at the same time (i.e.,

International Journal of Mathematical, Engineering and Management Sciences
Vol. 6, No. 1, 15-29, 2021
https://doi.org/10.33889/IJMEMS.2021.6.1.003

2 disks are in the vulnerable state and the remaining 2 disks are in either good or degradation state; or 2 disks are in the vulnerable state, 1 disk is in the failure state, and 1 disk is in either a good or a degradation state; or 3 disks are in the vulnerable state and the remaining 1 disk is in a good, or degradation, or failure state; or 4 disks are all in the vulnerable state). Any state other than the system good, vulnerable and failed states is considered as a degraded state for the example cloud RAID 5 system.

In the case of homogeneous disks, the probability of the system being in the good, vulnerable, and degraded states can be evaluated using Eqs. (12), (13), and (14) respectively.

$$P_{sys=0}(t) = C_4^3(P_0)^3(1- P_0) + C_4^4(P_0)^4, \quad (12)$$

$$P_{sys=2}(t) = C_4^2(P_2)^2(P_0 + P_1)^2 + C_4^2C_2^1(P_2)^2P_3(P_0 + P_1) + C_4^3(P_2)^3(1- P_2) + C_4^4(P_2)^4, \quad (13)$$

$$P_{sys=1}(t) = 1 - P_{sys=0}(t) - P_{sys=2}(t) - P_{sys=3}(t). \quad (14)$$

Based on the state probabilities evaluated using Eqs. (11)-(14), the survivability of the cloud RAID 5 system is given as,

$$S_{sys} = [1-P_{sys=3}(t)] = [P_{sys=0}(t) + P_{sys=1}(t) + P_{sys=1}(t)], \quad (15)$$

and the invulnerability of the system is given as,

$$I_{sys}= [1- P_{sys=2}(t) - P_{sys=3}(t)] = [P_{sys=0}(t)+ P_{sys=1}(t)]. \quad (16)$$

5. Disk-Level Analysis Results and Discussions

Based on statistics and survey reports from Avital et al. (2020), Check Point (2020), Hummel (2019), 11 sets of parameter values are designed for the transition rates in Figure 3 (Table 1), including the attack rates ρ_{gv}, ρ_{vf}, ρ_{gf} (number of attacks per hour), failure rates λ_{gd}, λ_{df}, λ_{gf} (number of failures per hour) and recovery rates μ_{dg}, r_{vg}, r_{fg} (number of repairs per hour).

Table 1. CTMC model parameters (per hour).

Rate	λ_{gd}	λ_{df}	λ_{gf}	ρ_{gf}	ρ_{gv}	P_{vf}	μ_{dg}	r_{vg}	r_{fg}
Set a	0.00015	0.0003	0.000018	0.00019	0.00091	0.037	0.2	0.16	0.057
Set b	0.00015	0.0003	0.000018	0.00019	0.0048	0.037	0.2	0.16	0.057
Set c	0.00015	0.0003	0.000018	0.00019	0.0136	0.037	0.2	0.16	0.057
Set d	0.00015	0.0003	0.000018	0.00019	0.167	0.037	0.2	0.16	0.057
Set e	0.00015	0.0003	0.000018	0.00019	3.1	0.037	0.2	0.16	0.057
Set f	0.00015	0.0003	0.000018	0.00019	0.0048	0.037	0.2	0.0011	0.057
Set g	0.00015	0.0003	0.000018	0.00019	0.0048	0.037	0.2	6.1	0.057
Set h	0.00015	0.0003	0.000018	0.00019	0.0048	0.037	0.2	77	0.057
Set i	0.00015	0.0003	0.000018	0.00019	0.0048	0.037	0.2	0.16	0.000027
Set j	0.00015	0.0003	0.000018	0.00019	0.0048	0.037	0.2	0.16	0.68
Set k	0.00015	0.0003	0.000018	0.00019	0.0048	0.037	0.2	0.16	74.9

Particularly, parameter ρ_{gv} refers to the frequency for a disk drive being attacked by DDoS attacks. According to the reports Avital et al. (2020), Hummel (2019), this rate can vary widely across several orders of magnitude from 8 attacks per year to 16 attacks per minute. According to Avital

International Journal of Mathematical, Engineering and Management Sciences
Vol. 6, No. 1, 15-29, 2021
https://doi.org/10.33889/IJMEMS.2021.6.1.003

et al. (2020), ρ_{gv} can be dependent on factors such as different industries (35.92% in Games, 2.95% in Finance), targeted countries (22.57% in India as the most, 8.73% in the United States) and habits of hackers. We choose the sets a, c, d, and e with the increasing rate values to study the impact of ρ_{gv} on the disk performance. The recovery rate r_{vg} reflects the different reactions in defending the system or device under the DDoS attacks; effects of this parameter on the disk performance are investigated through parameter sets f, b, g and h in Table 1. The survivability and invulnerability also depend on the network administrator's capability of handling network attacks or the quality of the existing cyber defense mechanism. For example, a cloud provider with an incident response plan would respond quickly and effectively after the crash with the occurrence of DDoS attacks; it can timely restore the server and keep the system functioning after attacks happen. The parameter r_{fg} model this recovery capability; its effects are investigated through parameter sets i, b, j and k in Table 1.

5.1 Effects of DDoS Attack Rate ρ_{gv}

Figure 6 plots the different state probabilities (P0, P1, P2 and P3) for the disk subject to DDoS attacks and disk faults for different values of attack rate ρ_{gv} (sets a, c, d, and e in Table 1) at different time points (from 0 to 54 hours). Among the four sets, ρ_{gv} in set a corresponds to the disk with the highest security level which has seldom been targeted. In contrast, ρ_{gv} in set e corresponds to another extreme case of being in the top attacked environment. ρ_{gv} in sets c and d correspond to intermediate cases between set a and set e.

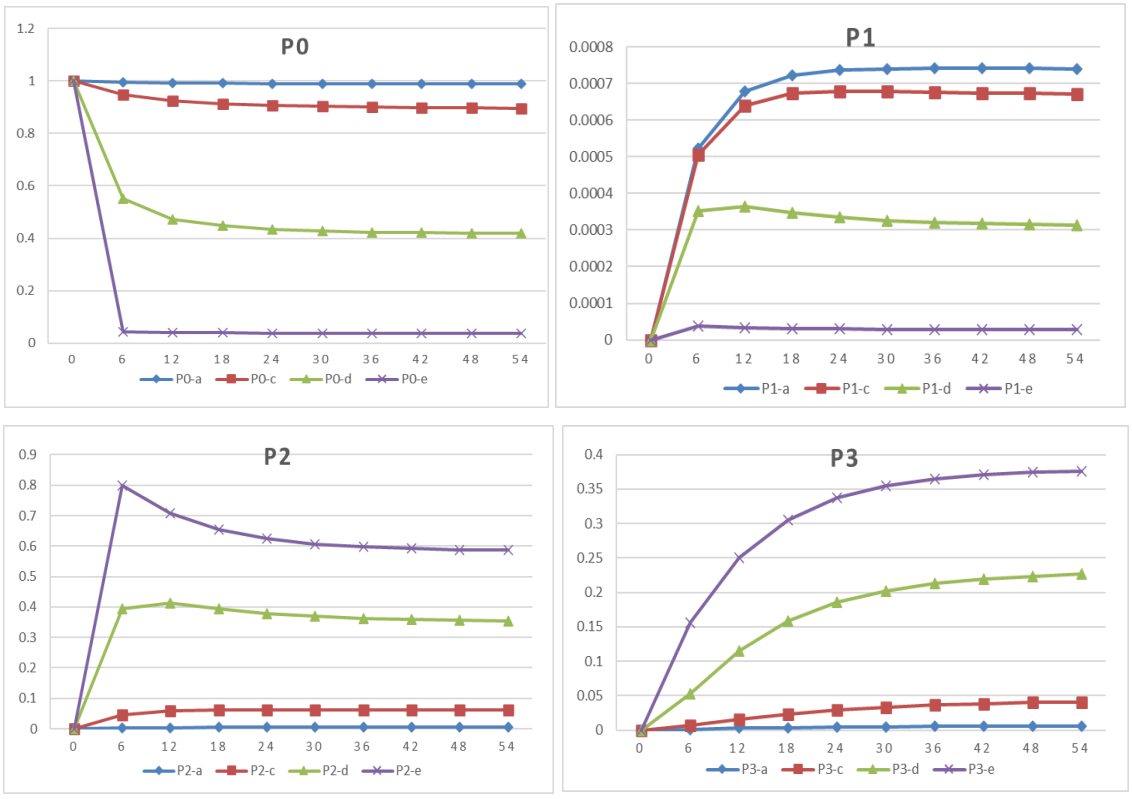

Figure 6. Probabilities of each disk state for different DDoS attack rates ρ_{gv} (x-axis: mission time t).

It is intuitive that the good state probability is decreasing with time. The good state probability under sets a and c falls very slowly as time proceeds due to small values of ρ_{gv}; while this probability under set e drops very quickly in the first 6 hours and then keeps the lowest over the considered mission time. Due to the complicated interactions among the transition rates, the trends for degradation state probability P1 and vulnerable state probability P2 appear non-monotonic under each considered parameter set, reaching a peak with a different pace, and then dropping gradually. In particular, P2-e stays the highest all the time and reaches the zenith 0.8 at t=6 hours while P2-a keeps the lowest over the considered mission time reaching its own peak until t=42 hours. The turning point (i.e., the time when the peak value is reached) for P2-c is t=24 hours and for P2-d is t=12 hours. Thus, as the attack rate increases, the turning point appears earlier. Conversely, P1-e remains the lowest reaching a peak value around t=6 hours due to the high-frequency DDoS attack while P1-a is the largest one and reaches its peak at t=42 hours. It can be observed that P1 and P2 share the same turning point under each parameter set. In addition, the values of P1 do not vary much under the different values of ρ_{gv}, implying that the rate ρ_{gv} affects the probabilities of states 0, 2 and 3 more than the probability of state 1. The failure state probability P3 shows an upward trend as time proceeds. It is intuitive that both the survivability (1-P3) and the invulnerability (1-P2-P3=P0+P1) appear the highest under set a (the smallest attack rate).

5.2 Effects of Recovery Rate r_{vg}

The survivability and vulnerability of the system are also related to the administrator's capability to cope with attacks-targeted system or defense capabilities of the system itself. This capability is modeled by the recovery rate r_{vg}. Its effects are investigated through the analysis under four parameter sets f, b, g and h listed in Table 1. Particularly, r_{vg} in set h models the strong recovery capability (an expert protects the disk with effective anti-virus/attack tool); r_{vg} in set f models a weak recovery capability (an amateur user); sets b and g model intermediate cases.

Figure 7 plots the different disk state probabilities under parameter sets f, b, g and h. It can be observed that the recovery rate r_{vg} impacts the good (0) and vulnerable (2) state probabilities more significantly than states 1 and 3. The good state probability P0 under set f (weak recovery capability) declines more quickly within 36 hours while P0 under sets g and h decreases much more slightly and then reaches the stable level around 0.995.

P1 and P3 both demonstrate the growing trend as time proceeds with slight differences for the four cases compared. It is intuitive that P2 under set h (the highest recovery rate) is the lowest (close to 0) due to the effective recovery action, while P2 under set f (the smallest recovery rate) grows significantly and is the largest one among the four cases compared. Due to the complicated interactions among the different transition rates, while the survivability (1-P3) is the largest, the invulnerability (1-P2-P3=P0+P1) appears the lowest under set f.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 6, No. 1, 15-29, 2021
https://doi.org/10.33889/IJMEMS.2021.6.1.003

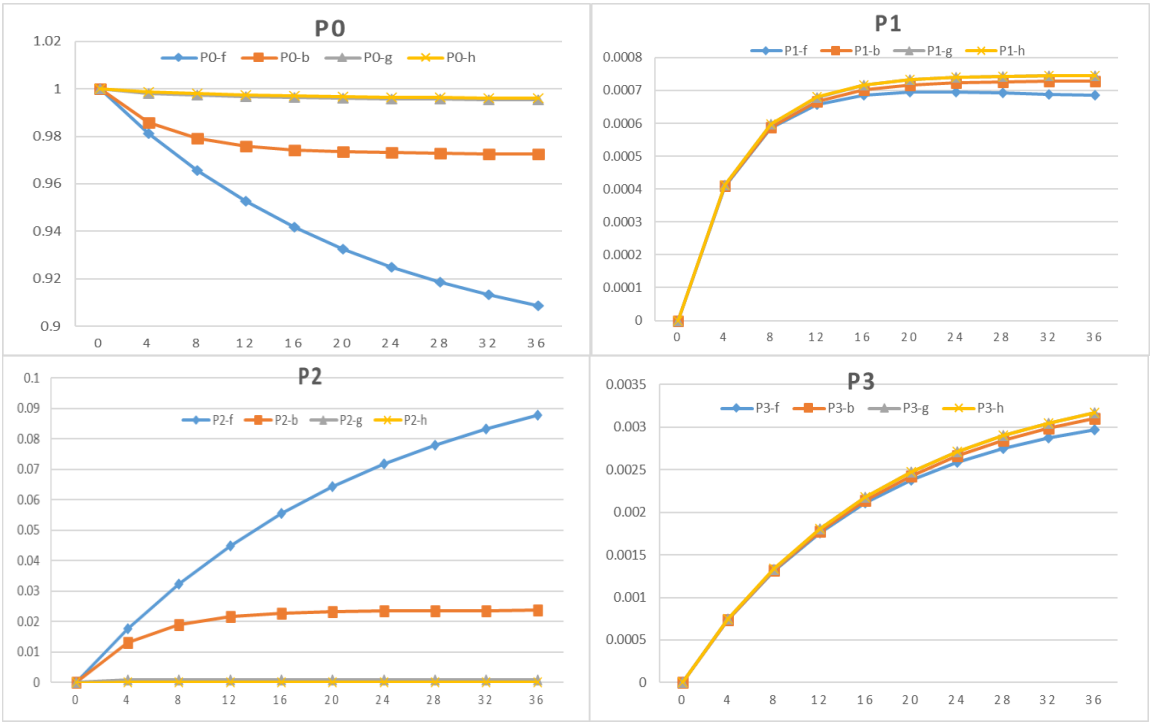

Figure 7. Probabilities of each disk state for different recovery rates r_{vg} (x-axis: mission time).

5.3 Effects of Rescue Rate r_{fg}

In the real life, there are several DDoS mitigation solutions according to Ahmed and Kim (2017) and Osanaiye et al. (2016), including for example using spare bandwidth, creating a DDoS action plan, improving the security of Internet of Things devices, monitoring traffic levels, or choosing a hosting provider who can give you DDoS protection as a service. In this section, we investigate effects of different mitigation mechanisms after the crash caused by DDoS attacks, which is modeled by parameter r_{fg}.

Figure 8 illustrates each disk state probability in the period of 0 to 24 hours under four sets i, b, j, k with varying values of r_{fg}. Among these four sets, set k with the highest rescue rate corresponds to cases where contingency strategies are performed regularly, leading to the lowest failure state probability P3 or the highest disk survivability and invulnerability. P3 under set i with the lowest rescue rate increases more significantly as the time proceeds than the other three sets and appears the highest. In addition, it can be observed that r_{fg} affects P0 and P3 more than P1 and P2 (where very slight differences are generated under the four sets i, b, j, k).

International Journal of Mathematical, Engineering and Management Sciences
Vol. 6, No. 1, 15-29, 2021
https://doi.org/10.33889/IJMEMS.2021.6.1.003

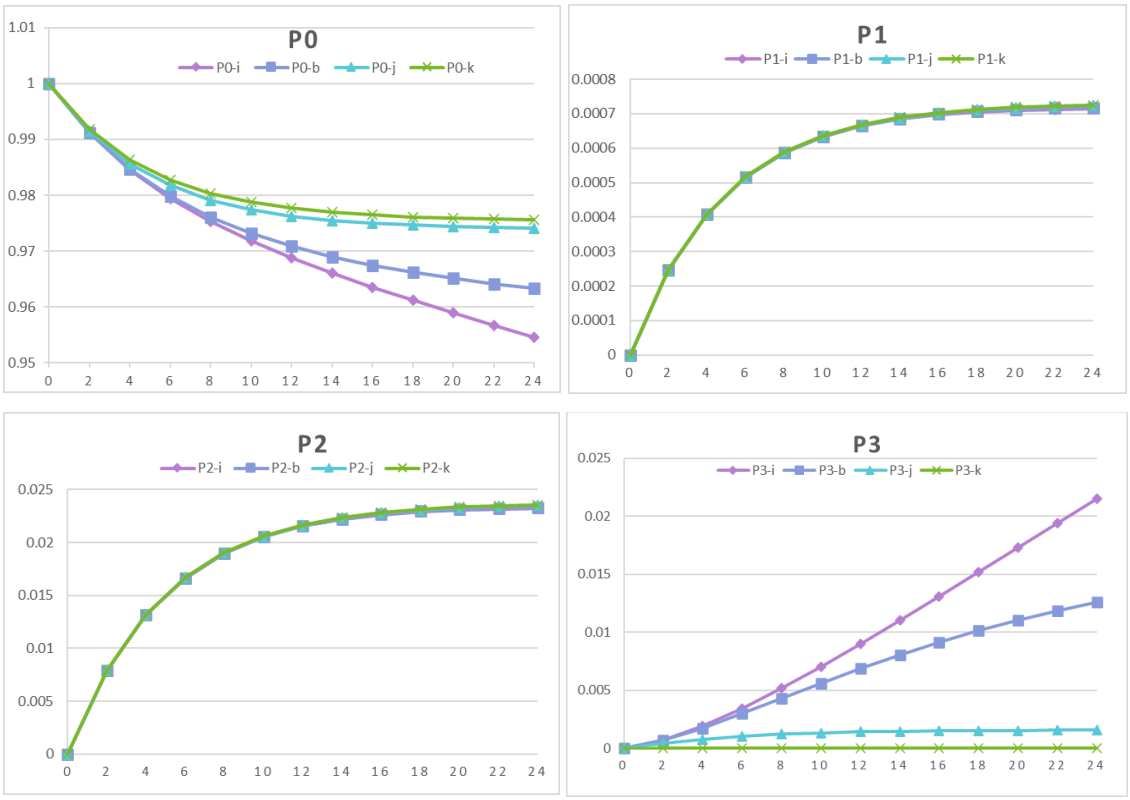

Figure 8. Probabilities of each disk state for different rescue mechanisms r_{fg} (x-axis: mission time).

6. System-Level Analysis Results and Discussions

Based on the equations derived in Section 4.2, Figures 9, 10 and 11 plot the system survivability and invulnerability to show the effects of parameters ρ_{gv}, r_{vg}, r_{fg}, respectively. All the empirical results supported the intuition that the system survivability decreases as time proceeds in all the cases. Moreover, the system invulnerability decreases as the attack rate increases, and it increases as the recovery or rescue rate increases.

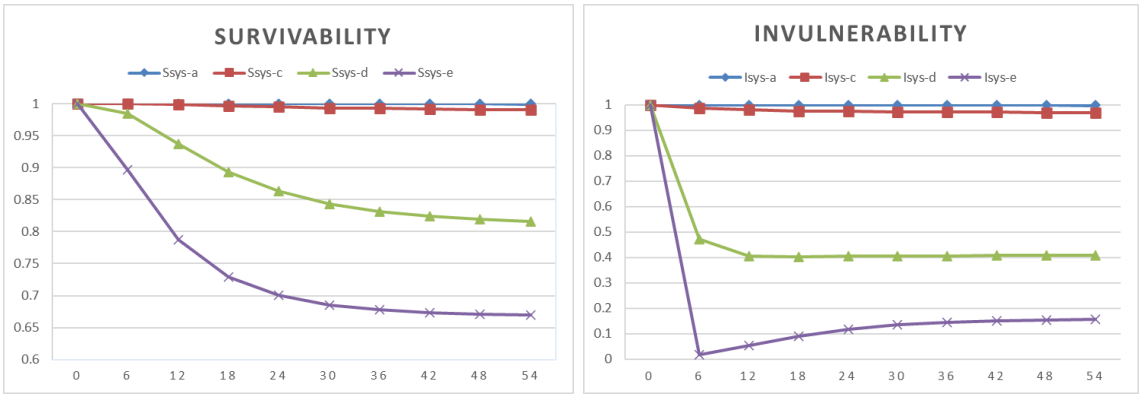

Figure 9. System survivability and invulnerability under different ρ_{gv} (x-axis: mission time).

International Journal of Mathematical, Engineering and Management Sciences
Vol. 6, No. 1, 15-29, 2021
https://doi.org/10.33889/IJMEMS.2021.6.1.003

Figure 9 illustrates the intuitive result that the system survivability under set e $S_{sys\text{-}e}$ with the highest attack rate decreases more quickly than the system survivability under the other three sets a, c, and d, and remains the lowest all the time. $S_{sys\text{-}a}$ with the smallest attack rate remains the largest during the considered mission time. The system invulnerability under set a $I_{sys\text{-}a}$ is almost flat staying the highest (near 1) among the four cases compared due to the lowest attack rate. The system invulnerability under set e $I_{sys\text{-}e}$ appears non-monotonic, beginning with a sharp drop in the first six hours, reaching the bottom with a value of 0.0165, and then increasing gradually. $I_{sys\text{-}e}$ is the lowest among the four cases compared due to the highest attack rate.

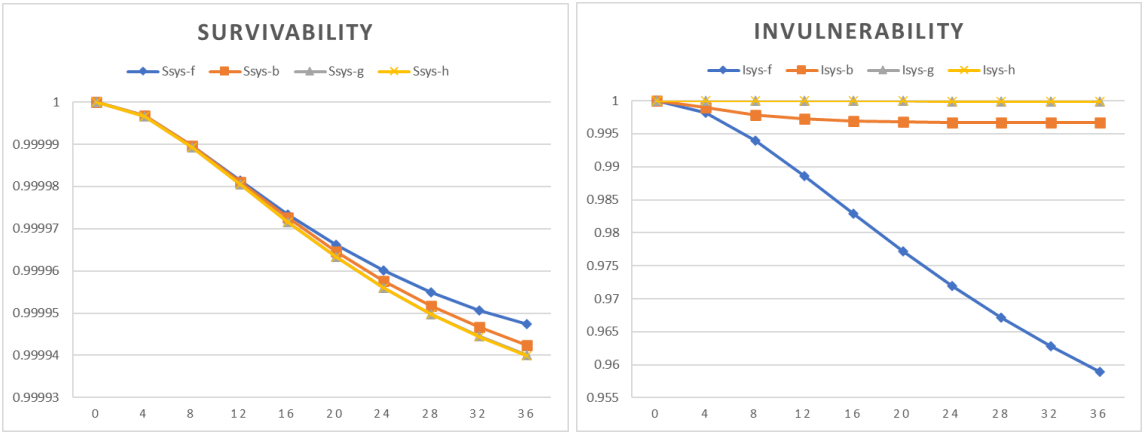

Figure 10. System survivability and invulnerability under different r_{vg} (x-axis: mission time).

It can be observed from Figure 10 that the system invulnerability under set h $I_{sys\text{-}h}$ with the highest recovery rate remains the largest level with subtle changes at different mission time while $I_{sys\text{-}f}$ under set f with the lowest recovery rate declines gradually from 1 to 0.958 during the considered mission time.

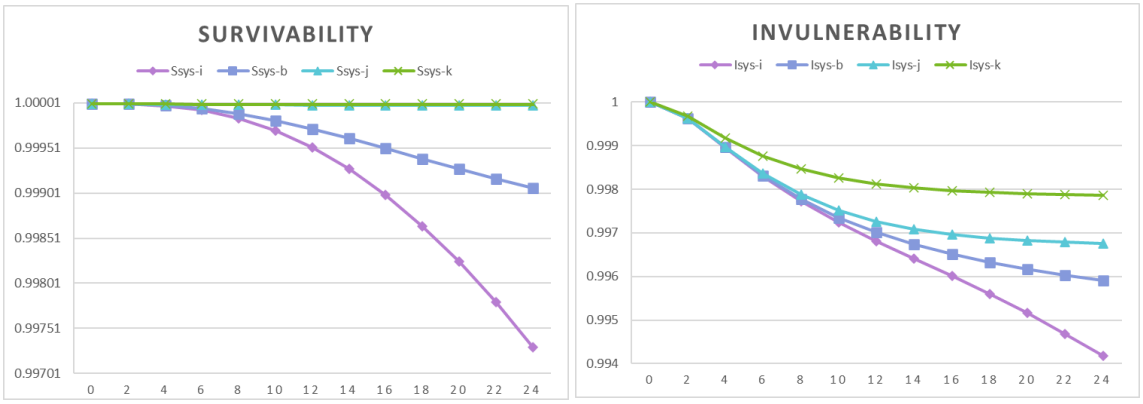

Figure 11. System survivability and invulnerability under different r_{fg} (x-axis: mission time).

It can be observed from Figure 11 that the system survivability $S_{sys\text{-}k}$ and invulnerability $I_{sys\text{-}k}$ under set k with the highest rescue rate appear the largest while $S_{sys\text{-}i}$ and $I_{sys\text{-}i}$ under set i with the lowest rescue rate are the lowest among the four sets compared. Because the rescue rate r_{fg} mainly affects the good state (0) and the failure state (3) of each disk, its impact on the system invulnerability is less than the impacts caused by changing ρ_{gv}, r_{vg} as shown in Figure 9 and 10.

7. Conclusions and Future Work

In this paper we suggest a survivability framework that enables the survivability and vulnerability modeling and analysis of cloud RAID storage systems considering both reliability and security threats. The quantitative assessment methods are then presented. Specifically, the CTMC-based method is used to analyze the disk level survivability and invulnerability. The combinatorial binomial coefficients-based and MDD-based methods are used to analyze the system level survivability and invulnerability in the case of homogeneous and heterogenous disks, respectively. Impacts of different attack and recovery parameters (particularly ρ_{gv}, r_{vg}, r_{fg}) on the disk and system survivability and invulnerability are investigated through the numerical analysis of an example cloud RAID 5 system.

The disk-level analysis method based on CTMCs is applicable to only the exponentially distributed state transition time. In the future, we are interested in investigating semi-Markov models or multiple integrals (Zeng et al., 2019) to accommodate non-exponential transition time distributions for disk state probability analysis. We are also interested in incorporating the sequential attack events for the survivability and invulnerability analysis of cloud storage systems.

Conflict of Interest

The authors confirm that there is no conflict of interest to declare for this publication.

Acknowledgments

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The authors would like to thank the editor and anonymous reviewers for their comments that help improve the quality of this work.

References

Ahmed, M.E., & Kim, H. (2017, April). DDoS attack mitigation in Internet of Things using software defined networking. In *2017 IEEE Third International Conference on Big Data Computing Service and Applications* (pp. 271-276). IEEE. San Francisco, CA.

Avital, N., Zawoznik, A., Azaria, J., & Lambert, K. (2020). *2019 global DDoS threat landscape report*. Imperva Research Labs, https://www.imperva.com/blog/2019-global-ddos-threat-landscape-report/, Accessed in May 2020.

Bamiah, M.A., & Brohi, S.N. (2011). Seven deadly threats and vulnerabilities in cloud computing. *International Journal of Advanced Engineering Sciences and Technologies*, *9*(1), 87-90.

Check Point. (2020). Security report 2020. *Check Point Software Technologies Ltd*, https://www.bristol.de/wp-content/uploads/2020/03/2020-security-report.pdf, Accessed in May 2020.

Chou, T.S. (2013). Security threats on cloud computing vulnerabilities. *International Journal of Computer Science & Information Technology*, *5*(3), 79.

Escudero, C., Sicard, F., & Zamaï, É. (2018, September). Process-aware model based IDSs for industrial control systems cybersecurity: approaches, limits and further research. In *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)* (Vol. 1, pp. 605-612). IEEE. Funchal, Portugal.

Fung, C., Chen, Y.L., Wang, X., Lee, J., Tarquini, R., Anderson, M., & Linger, R. (2005, October). Survivability analysis of distributed systems using attack tree methodology. In *MILCOM 2005-2005 IEEE Military Communications Conference* (pp. 583-589). IEEE. Atlantic City, NJ.

George, G., & Thampi, S.M. (2018, September). A graph-based decision support model for vulnerability analysis in IoT networks. In *International Symposium on Security in Computing and Communication* (pp. 1-23). Springer, Singapore.

Hasan, M.M., & Rahman, M.A. (2020). A signaling game approach to mitigate co-resident attacks in an IaaS cloud environment. *Journal of Information Security and Applications*, *50*, 102397.

Hummel, R. (2019). *Netscout threat intelligence report*. Netscout System INC, https://www.netscout.com/sites/default/files/2020-02/SECR_001_EN-2001_Web.pdf, Accessed in May 2020.

Iliadis, I., Sotnikov, D., Ta-Shma, P., & Venkatesan, V. (2014, November). Reliability of geo-replicated cloud storage systems. In *2014 IEEE 20th Pacific Rim International Symposium on Dependable Computing* (pp. 169-179). IEEE. Singapore.

Ko, R., Lee, S.G., & Rajan, V. (2013). Cloud computing vulnerability incidents: a statistical overview. *Cloud Security Alliance*, https://crow.org.nz/sites/default/files/2017-01/Cloud_Computing_Vulnerability_Incidents.pdf, Accessed in May 2020.

Levitin, G., Xing, L., & Dai, Y. (2018). Co-residence based data vulnerability vs. security in cloud computing system with random server assignment. *European Journal of Operational Research*, *267*(2), 676-686.

Liu, Q., & Xing, L. (2015a). Reliability modeling of cloud-RAID-6 storage system. *International Journal of Future Computer and Communication*, *4*(6), 415-420.

Liu, Q., & Xing, L. (2015b). Hierarchical reliability analysis of multi-state cloud-RAID storage system. In *Proc. of International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering* (pp. 1-7). Beijing, China.

Liu, Q., Xing, L., & Zhou, C. (2019). Probabilistic modeling and analysis of sequential cyber-attacks. *Engineering Reports*, *1*(4), e12065.

Mandava, L., & Xing, L. (2019). Balancing reliability and cost in cloud-RAID systems with fault-level coverage. *International Journal* of *Mathematical*, *Engineering* and *Management* Sciences, *4*(5), 1068-1080.

Mandava, L., & Xing, L. (2020). Optimizing imperfect coverage cloud-RAID systems considering reliability and cost. *International Journal of Reliability, Quality and Safety Engineering*, *27*(2), 2040001.

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39-53.

Nachiappan, R., Javadi, B., Calheiros, R.N., & Matawie, K.M. (2017). Cloud storage reliability for big data applications: a state of the art survey. *Journal of Network and Computer Applications*, *97*, 35-47.

Osanaiye, O., Choo, K.K.R., & Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework. *Journal of Network and Computer Applications*, *67*, 147-165.

Shahrad, M., Mosenia, A., Song, L., Chiang, M., Wentzlaff, D., & Mittal, P. (2018). Acoustic denial of service attacks on hard disk drives. In *Proc. of the 2018 Workshop on Attacks and Solutions in Hardware Security* (pp. 34–39). ACM, New York, USA, DOI: https://doi.org/10.1145/3266444.3266448.

Wang, B., Zheng, Y., Lou, W., & Hou, Y.T. (2015). DDoS attack protection in the era of cloud computing and software-defined networking. *Computer Networks*, *81*, 308-319.

Widder, D.V. (2015). *Laplace transform (PMS-6)*. Princeton university press. Princeton, NJ.

Xing, L. (2020). Reliability in Internet of Things: current status and future perspectives. *IEEE Internet of Things Journal*, in press, doi: 10.1109/JIOT.2020.2993216.

Xing, L., & Amari, S.V. (2015). *Binary decision diagrams and extensions for system reliability analysis*. Scrivener Publishing LLC, Beverly, MA and Wiley, doi:10.1002/9781119178026.

Xing, L., & Dai, Y.S. (2009). A new decision-diagram-based method for efficient analysis on multistate systems. *IEEE Transactions on Dependable and Secure Computing*, *6*(3), 161-174.

Xing, L., Levitin, G., & Xiang, Y. (2019). Defending N-version programming service components against co-resident attacks in IoT cloud systems. *IEEE Transactions on Services Computing*, doi: 10.1109/TSC.2019.2904958.

Xu, S., Yang, G., Mu, Y., & Liu, X. (2019). A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance. *Future Generation Computer Systems*, *97*, 284-294.

Zeng, Y., Xing, L., Zhang, Q., & Jia, X. (2019). An analytical method for reliability analysis of hardware-software co-design system. *Quality and Reliability Engineering International*, *35*(1), 165-178.

Zhang, R., Lin, C., Meng, K., & Zhu, L. (2013, November). A modeling reliability analysis technique for cloud storage system. In *2013 15th IEEE International Conference on Communication Technology* (pp. 32-36). IEEE. Guilin, China.