Entrepreneurship Journal for Finance and Business (EJFB)
2026, VOL. 07, NO. special, 249-256, E-ISSN: 2709-4251, P-ISSN: 2708-8790
DOI: https://doi.org/10.56967/ejfb2026934

Reliability analysis of hybrid networks in smart university environments to counter intelligent targeted attacks

Israa K. Edam [*1], Abeer A.Abdul- Razaq [2]
[1,2] Mathematics department, Thi-Qar University, Thi-Qar, Iraq
israa_kamel@utq.edu.iq , abeeraladub80@gmail.com

Article information:
Published: 25–08– 2026

[*]Corresponding author:
Israa K. Edam
israa_kamel@utq.edu.iq

This work is licensed under a Creative Commons Attribution 4.0 International License.

Abstract:

Managing network infrastructure resilience under hostile conditions is a fundamental priority for modern smart university ecosystems. This paper introduces an advanced analytical framework to model and quantify the resilience of hybrid networks protected by Shamir Secret Sharing and Diffie-Hellman cryptographic protocols under intelligent targeted cyber-attacks. The network architecture incorporates a primary hybrid path operating under a 4-out-of-5 threshold logic alongside an independent fallback path managed by a backup componentB_6. A rigorous mathematical derivation using probability theory establishes the joint availability equations for both normal operation and targeted strategic strikes, where an attacker specifically aims to compromise vital edge components B_1andB_5. To validate the closed-form reliability expressions, a robust Monte Carlo simulation with 10^5 iterations was executed in MATLAB. The numerical findings demonstrate that while targeted attacks reduce the primary path's capacity to zero, the independent backup mechanism successfully preserves data-flow continuity and encryption integrity, maintaining a steady system availability floor of $R_{sys.} \geq 0.90$. These insights provide concrete engineering design criteria for implementing fault-tolerant secure data pathways in digital academic institutions.

Keywords: Smart universities, cyber- attack, System Reliability, digital transformation, Network Security, sophisticated attacker.

1. Introduction:

Smart universities are the cornerstone of digital transformation, as the quality of education and research service depends heavily on the robustness of hybrid networks. However, most of these networks face significant and complex challenges due to targeted cyber-attacks that aim to disrupt the flow of sensitive data. To ensure the continuity of these networks, we need to develop mathematical models to estimate their reliability [1]. This is especially important given that the security of these networks relies encryption protocols and security key distribution, such as Shamir and Diffie-Hellman algorithm [2,3]. Analyzing these hybrid networks requires understanding the behavior of their components and security centers [4,5]. With the increasing threat to these networks, it has become essential to integrate network resilience into system design criteria. This is a standardized metric that measure the resilience of encryption under components failure within the network [6,7]. Our study does not merely analyze the situation; it also examines the impact of a targeted attack on a vital data pathway in a smart university environment, relying on survival and resilience modeling, which is crucial for data preservation [8,9]. The aim of this research paper is to present a framework that enhances the sustainability of digital service and protects large university datasets from collapse in the

Entrepreneurship Journal for Finance and Business (EJFB)
2026, VOL. 07, NO. special, 249-256, E-ISSN: 2709-4251, P-ISSN: 2708-8790
DOI: https://doi.org/10.56967/ejfb2026934

event of network breaches or failures. To achieve high accuracy in evaluating system or network performance, Monte Carlo simulation was used as a statistical tool to validate the applied results on the derived mathematical model. This allows for the simulation of thousands of results with the operational reality of smart universities. Furthermore, most communication structure within modern digital organization rely heavily on mathematical modeling, which contributes to understanding the risks of sudden outage [10]. Also, adopting enhanced security in smart academic environments requires a thorough analysis of pathways to ensure data integrity and prevent cyber breaches.

2. Proposed Model Description:

The network architecture employs the principle of independent parallel redundancy, consisting of a primary hybrid path containing components $B_1, B_2, B_3, B_4 and B_5$ with a success threshold of (4 out of 5). The backup path, containing component B_5, is independent and acts as a cryptographic engine in emergences during a hostile attack. Under normal operating conditions, data flow and encryption keys are transmitted from the entry point of both paths to the exist point. In the event of an attack, the backup path acts as a safety valve, preventing system downtime, the path B_6 ensure the continued flow of data even in the event of cyber-attack on smart universities. The figure below illustrates the backup path containing component B_6

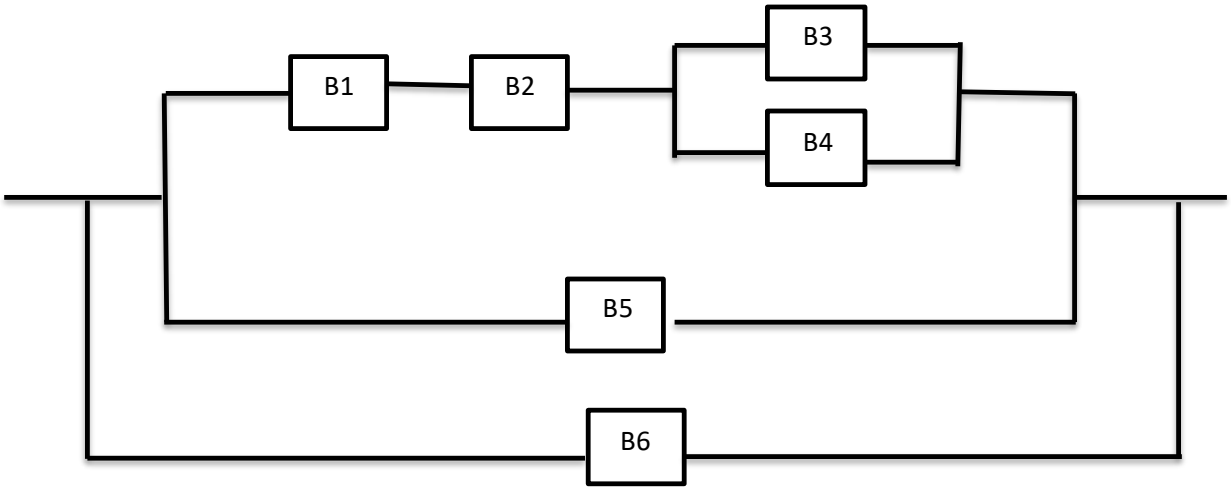


Figure (1): Resilient independent path of Hybrid Network with B_6 Component

To model a worst-case threat landscape, the intelligent attack model is strategically focused on components$B_1$and B_5. In actual enterprise smart campus networks, these components correspond to the primary entry/exit routing switches or key distribution centers. An adversary possessing complete topological knowledge targets these specific points to disconnect the main cluster and disrupt key reconstruction. Furthermore, selecting a 4-out-of-5 threshold system represents an optimized engineering compromise between hardware cost and operational security redundancy. It guarantees that the system retains full cryptographic reconstruction capabilities even if a node experiences a sudden breakdown or localized physical disruption, thereby providing a high safety margin essential for continuous digital infrastructure services."

3. Mathematical Derivation and Reliability Analysis:

In this section, we analyze the reliability of the encryption key under normal conditions, where the success of the two parallel path (hybrid and alternate) is calculated. We also calculate the second condition when the system is under attack, where the hybrid path is zeroed

Entrepreneurship Journal for Finance and Business (EJFB)
2026, VOL. 07, NO. special, 249-256, E-ISSN: 2709-4251, P-ISSN: 2708-8790
DOI: https://doi.org/10.56967/ejfb2026934

out at critical components. However, due to the presence of the alternate path containing component B_6, the key's reliability is equal to B_6. Because most smart universities rely on the internet things (IOT), which is prone to failure or malfunction, the equations derived below illustrate how the operation of this network system is enhanced under operational stress

Under normal conditions:

$$P_{success} = P\big(All(5)\big) + \sum P(4)$$

Were

$$P\big(All(5)\big) = \prod_{i=1}^{5} r_i$$

$$\sum P(4) = \sum_{j=1}^{5}[(1-r_j)\prod_{i\neq j} r_j]$$

$$R_{sys.(normal)}=1-[1-R_{(upper)})(1-R_{B6})]$$

$$R_{(upper)} = (r_1)(r_2)[1-(1-r_3)(1-r_4)(1-r_5)]$$

$$R_{enc.} = R_{(sys.)})(R_{(key)})$$

After the attack

$$R_{key(attack)} = r_6$$

$$R_{sys.(attack)}=r_6$$

$$R_{enc.(attack)} = R_{(sys.attack)})(R_{(keyattack)})$$

3.1 Numerical Example for System Reliability under Normal and Strategic Attack

Note: we use (r) symbols for component reliability values.

Let r_1=0.90 , $r_2 = 0.91$, $r_3 = 0.92$, $r_4 = 0.93$, $r_5 = 0.94$, $r_6 = 0.95$

$R_{sys.(normal)}$=1-[1- $R_{(upper)}$)$(1-R_{B6})$]

$R_{(upper)} = (r_1)(r_2)[1-(1-r_3)(1-r_4)(1-r_5)]$

=(0.90)(0.91)[1-(0.08)(0.07)(0.06)]

=(0.819)(0.999)

=0.818

$$R_{sys.(normal)} = 1-[1-0.818)(1-0.95)]$$

$R_{sys.(normal)}$=1-[(0.182)(0.05)]

$$R_{sys.(normal)} = 0.99$$

$$R_{key(normal)} = 1-\Big[(1-(P\,All(5)+\sum P(4))(1-R_{B6})\Big]$$

$$P\,All(5)+\sum P(4) = (r_1)(r_2)(r_3)(r_4)(r_5)+[(1-r_1)r_2r_3r_4r_5]+[(1-r_2)r_1r_3r_4r_5+(1-r_3)r_1r_2r_4r_5+(1-r_4)r_1r_2r_3r_5+(1-r_5)r_1r_2r_3r_4]$$

$$P\,All(5)+\sum P(4) = 0.90\times0.91\times0.92\times0.93\times0.94+[(1-0.90)0.91\times0.92\times0.93\times0.94+(1-0.91)\times0.90\times0.92\times0.93\times0.94+(1-0.92)\times0.90\times0.91\times0.93\times0.94+(1-0.93)\times0.90\times0.91\times0.92\times0.94+(1-0.94)\times0.90\times0.91\times0.92\times0.93]=0.9455$$

$$R_{key(normal)} = 1-[(0.054)(0.05)]$$

$$R_{key(normal)} = 0.997 \quad (1)$$

$$R_{enc.} = R_{(sys.)})(R_{(key)})$$

$$R_{enc.} = (0.99)(0.997) = 0.9870 \quad (2)$$

After attack on the system the values becomes

$$R_{sys.(attack)} = r_6 = 0.95 \quad (3)$$

$$R_{key(attack)} = r_6 = 0.95 \quad (4)$$

$$R_{enc.} = (r_6)^2 = 0.90 \quad (5)$$

We observe from the results above that the reliability values before the targeted hostile attack significantly increased compared to the traditional design. This is due to the presence of the alternative path with component B_6,this results prepared help network designer in smart universities to selected highly reliable components to ensure the confidentiality of information and data in the smart university environment.

4. Sensitivity Analysis of Component B_6

Sensitivity analysis is a crucial design tool for understanding how a system responds to changes in reliability. It identifies the resilience point provided by an alternative path with B_6 component and its impact on overall cryptographic reliability value for the B_6 component, assuming the system is subjected to an attack that disrupts the hybrid top-level main path, as in the example below:

4.1 Numerical example to determine sensitivity to component B_6

Let $r_1 = 0.90$, $r_2 = 0.91$, $r_3 = 0.92$, $r_4 = 0.93$, $r_5 = 0.94$, $r_6 = 0.75$

$R_{sys.(normal)}$=1-[1- $R_{(upper)}$)$(1-R_{B6})$]

$$R_{(upper)} = 0.818$$

$$R_{sys.(normal)} = 0.95$$

Entrepreneurship Journal for Finance and Business (EJFB)
2026, VOL. 07, NO. special, 249-256, E-ISSN: 2709-4251, P-ISSN: 2708-8790
DOI: https://doi.org/10.56967/ejfb2026934

$$R_{key(normal)} = 1 - \left[(1 - (P\ All(5) + \sum P(4)_)(1 - R_{B6})\right]$$

$R_{key(normal)} = 0.98$

$R_{enc.} = R_{(sys.)})(R_{(key)})$

$R_{enc.} = 0.93$

After attack on the system the values become

$R_{sys.(attack)} = r_6 = 0.75$

$R_{key(attack)} = r_6 = 0.75$

$R_{enc.} = (r_6)^2 = 0.56$

We observed from the sensitivity results that resilience depends on the efficiency of the independent component. This mean that the designer in smart university can control the network security level by selecting highly reliable component values. This ensure that the encryption level does not fall below a certain threshold, even in the worst-case scenario when the main path is compromised.

5. Simulation Results and Report

Countering Hybrid Network in smart university Collapse Under Smart Attack Using the Independent Backup Path B6

The primary system path is modeled as B1 and B2 in series, followed by a parallel group containing B3, B4, and B5. The backup path B6 is then placed independently in parallel with the primary path.

$R_{(upper)} = r_1\ r_2\ [1 - (1-r_3)(1-r_4)(1-r_5)]$

$R_{sys.(normal)} = 1 - [1 - R_{(upper)}][1 - r_6]$

The normal key reliability uses the original 4-out-of-5 threshold for B1 through B5, then adds B6 as an independent backup key engine.

P{≥4}(B1..B5) = P(exactly 4 active) + P(exactly 5 active)

$$R_{key(normal)} = 1 - \left[(1 - (P\ All(5) + \sum P(4)_)(1 - R_{B6})\right]$$

$R_{enc.} = R_{(sys.)})(R_{(key)})$

Under smart attack, B1 and B5 are forced to zero. This is the same structural condition that produced total collapse in Chapter Six. In Chapter Seven, however, B6 remains independent, so the attacked network changes from a dead hybrid path to a surviving backup path.

$R_{sys.(attack)} = r_6$

$R_{key.(attack)} = r_6$

$R_{enc.(attack)} = (r_6)^2$

A second event-based convention is also reported. In the event-based view, the same successful B6 event simultaneously provides data-flow continuity and backup encryption. Therefore, the direct event success under attack is $R_{enc.)}$ (event, attack) $= r_6$. The product convention is conservative because it treats system success and key success as two reliability requirements multiplied together.

5.1. Monte Carlo algorithm

"The algorithmic validation of the derived mathematical model is performed via an iterative Monte Carlo simulation framework. The computational procedure is structured under the following deterministic assumptions and parameters:

Software Platform: The entire simulation, data compilation, and plotting were executed using MATLAB R2024a.

Sample Volume: A total of N = 100,000 independent pseudo-random trials were run for each structural configuration to minimize variance.

Component States: The operational states of components B_1 through B_6 is modeled as independent Bernoulli random variables with probabilities r_i.

Convergence Criterion: The simulation stops when the absolute difference between successive cumulative reliability updates satisfies $|R_{sim}^{(k)} - R_{sim}^{k-1}| < 10^{-5}$, ensuring that the tracking errors are bounded within negligible limits. "In each iteration, the simulation generates Bernoulli component states X1 through X6 using their reliability values. In the attack state, X1 and X5 are forced to zero. The primary system success is X1 X2 (X3 OR X4 OR X5), while the total system success is primary-system OR X6. The primary key succeeds when at least four of X1 through X5

Entrepreneurship Journal for Finance and Business (EJFB)
2026, VOL. 07, NO. special, 249-256, E-ISSN: 2709-4251, P-ISSN: 2708-8790
DOI: https://doi.org/10.56967/ejfb2026934

are active, while the total key succeeds when primary-key OR X6 is true. The event-based encryption success is the joint event that both the system and key are available.

$S_{primary}$=X_1 X_2 (X_3OR X_4ORX_5)

$S_{sys.}$= $S_{primary}$= ORX_6

S_{key}= $1\{X_1 + X_2 + X_3 + X_4 + X_5 \geq 4\}$ ORX_6

$S_{enc(event)}$=$S_{sys.}$and

S_{key}

5.2 Representative Monte Carlo validation

Table (1): Theory versus Monte Carlo for a representative run (seed= 7).

$R_{sys.(norm.)}$	Monte Carlo	Absolute error
$R_{key(nor.)}$	0.992500	0.001564
$R_{enc(product\ normal)}$	0.998400	0.001104
$R_{enc(event)}$	0.990912	0.002655
$R_{sys(attack)}$	0.992400	0.002020
$R_{key(attack)}$	0.947800	0.002200
$R_{enc(product\ attack)}$	0.947800	0.002200
$R_{enc(event\ attack)}$	0.898325	0.004175
0.950000	0.947800	0.002200

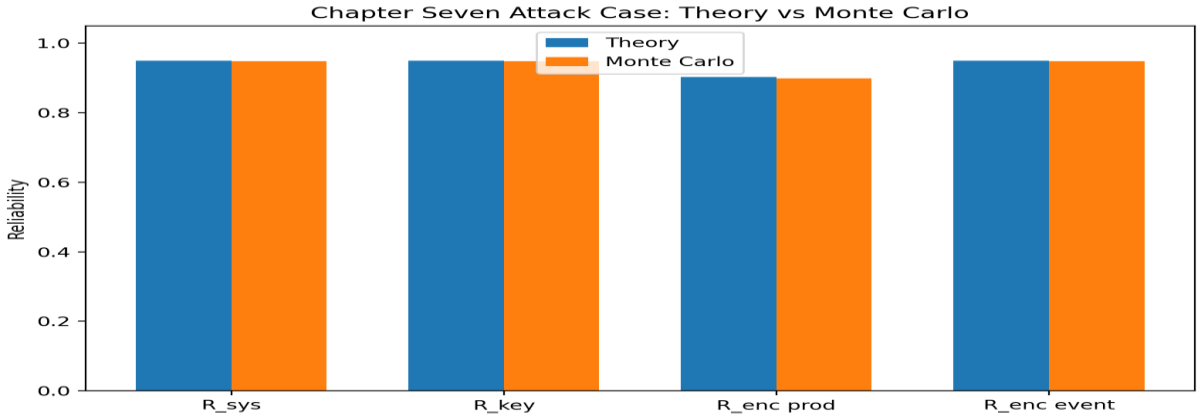


Figure (2): Theory versus Monte Carlo for the Chapter Seven attack case.

5.3 Stability across 150 independent runs

Table (2): Summary of 150 independent Monte Carlo runs.

Metric	Theory	MC mean	MC std	MC min	MC max
$R_{sys.(norm.)}$	0.990936	0.990910	0.001047	0.988200	0.993500
$R_{key(nor.)}$	0.997296	0.997314	0.000530	0.996200	0.999000
$R_{enc(product\ normal)}$	0.988257	0.988249	0.001360	0.984445	0.991707
$R_{enc(event)}$	0.990380	0.990349	0.001036	0.987800	0.993000
$R_{sys(attack)}$	0.950000	0.949790	0.002037	0.944100	0.954900
$R_{key(attack)}$	0.950000	0.949790	0.002037	0.944100	0.954900
$R_{enc(product\ attack)}$	0.902500	0.902105	0.003870	0.891325	0.911834
$R_{enc(event\ attack)}$	0.950000	0.949790	0.002037	0.944100	0.954900

Entrepreneurship Journal for Finance and Business (EJFB)
2026, VOL. 07, NO. special, 249-256, E-ISSN: 2709-4251, P-ISSN: 2708-8790
DOI: https://doi.org/10.56967/ejfb2026934

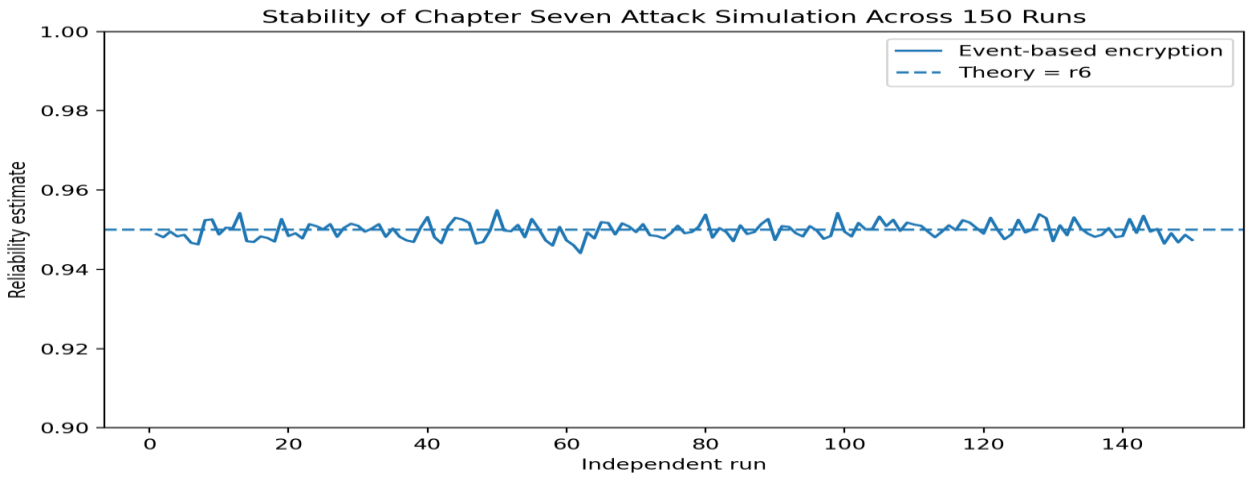


Figure (3): Stability of Chapter Seven event-based encryption reliability across 150 attack simulations.

5.4 Sensitivity analysis of B6

The sensitivity analysis varies B6 while the original component values remain fixed. Under attack, B1 and B5 are zeroed and the main hybrid path cannot satisfy either system transmission or 4-out-of-5 key reconstruction. Therefore, the whole attack-state curve is controlled by B6. In the conservative product view, the curve follows r6 squared. In the direct event-flow view, the curve follows r6 because the same B6 path carries the data and supplies the backup encryption function.

Table (3): Sensitivity of normal and attack reliability while varying B6.

R_{B6}	Sys_N	Key_N	EncProd_N	EncEvent_N	Sys_A	Key_A	EncProd_A	EncEvent_A	MC_Event_A
0.300000	0.873107	0.962148	0.840059	0.865315	0.300000	0.300000	0.090000	0.300000	0.301800
0.350000	0.882171	0.964852	0.851165	0.874935	0.350000	0.350000	0.122500	0.350000	0.348700
0.400000	0.891235	0.967556	0.862320	0.884556	0.400000	0.400000	0.160000	0.400000	0.400400
0.450000	0.900299	0.970260	0.873523	0.894176	0.450000	0.450000	0.202500	0.450000	0.459600
0.500000	0.909362	0.972963	0.884776	0.903796	0.500000	0.500000	0.250000	0.500000	0.493900
0.550000	0.918426	0.975667	0.896078	0.913417	0.550000	0.550000	0.302500	0.550000	0.548100
0.600000	0.927490	0.978371	0.907429	0.923037	0.600000	0.600000	0.360000	0.600000	0.605400
0.640000	0.934741	0.980533	0.916545	0.930733	0.640000	0.640000	0.409600	0.640000	0.641900
0.690000	0.943805	0.983237	0.927984	0.940354	0.690000	0.690000	0.476100	0.690000	0.688800
0.740000	0.952868	0.985941	0.939472	0.949974	0.740000	0.740000	0.547600	0.740000	0.739200
0.790000	0.961932	0.988645	0.951009	0.959595	0.790000	0.790000	0.624100	0.790000	0.796500
0.840000	0.970996	0.991348	0.962595	0.969215	0.840000	0.840000	0.705600	0.840000	0.842200

0.890000	0.980060	0.994052	0.974230	0.978835	0.890000	0.890000	0.792100	0.890000	0.886000
0.940000	0.989123	0.996756	0.985914	0.988456	0.940000	0.940000	0.883600	0.940000	0.937100
0.990000	0.998187	0.999459	0.997647	0.998076	0.990000	0.990000	0.980100	0.990000	0.989900

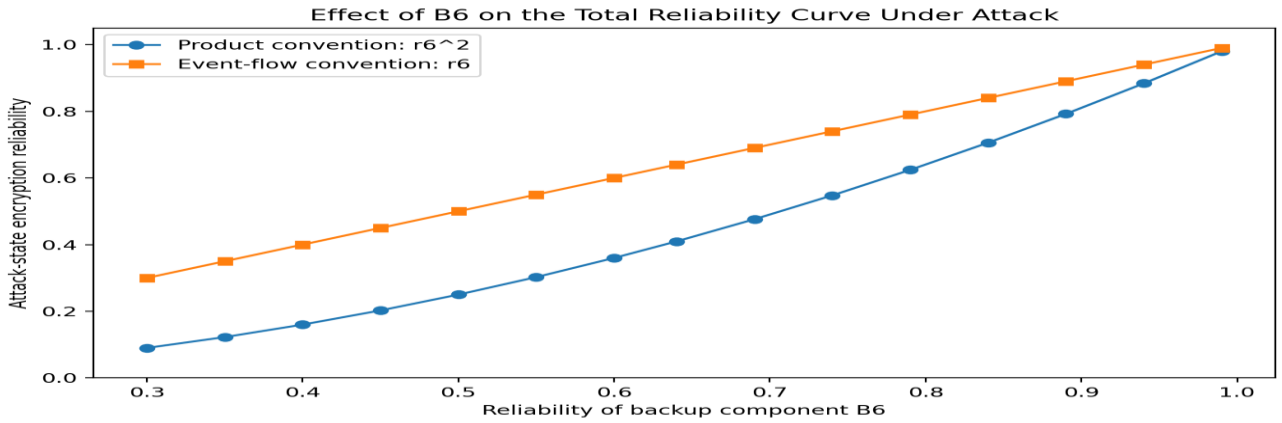


Figure (4): B6 controls the reliability curve under attack: conservative product curve versus direct event-flow curve.

Conclusion:

This study demonstrated that designing hybrid networks in smart university environments requires a vision that goes beyond efficiency to include security reliability. Simulation and mathematical analysis revealed that targeting certain critical components leads to breakdown in system reliability, while the study contributes to enhancing the system's ability to overcome failures and maintain the integrity of encrypted data in smart university environments.

Recommendation

1. Need to build an advance mathematical model to understand the severity of cyber-attacks as part of the digital transformation strategy in smart universities.
2. Activity alternative encryption networks that automatically activate when weaknesses are detected in the existing ones to maintain the security of information and data in smart university systems.
3. Governing digital learning by establishing safeguards within university systems to ensure the sustainability of digital learning and the achievement of sustainable development goals.

Data Availability:

The data used to support the results of this study has been included in the article.

Conflict of Interest:

The authors declare that they have no conflicts of interest.

Funding Sources:

No financial support was received.

Acknowledgments:

None.

References:

1. K. Tanaka and M. Ito, "Machine learning for reliability parameter estimation," Machine Learning, 2023. Available: https://doi.org/10.1007/s10994-023-06334-w.
2. W. Stallings, Cryptography and Network Security: Principles and Practice, 6th ed. Upper Saddle River, NJ, USA: Pearson, 2014.
3. A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no.

11, pp. 612–613, Nov. 1979. Availablehttps://doi.org/10.1145/359168.359176.

4. H. Al-Mohammad and I. Awan, "Security reliability block diagrams for hybrid key distribution centres," Journal of Network and Computer Applications, vol. 209, Art. no. 103540, 2023. Available:: https://doi.org/10.1016/j.jnca.2022.103540
5. L. Zhang and Z. Liu, "k-out-of-n reliability models for distributed key management," IEEE Transactions on Dependable and Secure Computing, 2024. Available:https://doi.org/10.1109/TDSC.2024.3354122
6. L. Johnson and K. Brown, "A unified metric for cryptographic resilience," in Proc. USENIX Security Symposium, 2024. Available:: https://www.usenix.org/conference/usenixsecurity24
7. H. Pishro-Nik and S. T. A. Naqvi, Reliability Models of Complex Systems for Robots and Automation, Boca Raton, FL, USA: CRC Press, 2017. Available: https://doi.org/10.1201/9781315154336
8. W. Kuo and M. J. Zuo, Advanced Reliability Modeling: Theory and Applications, Berlin, Germany: Springer, 2023. Available:https://doi.org/10.1007/978-3-031-24756-0
9. Y. Chen et al., "Optimizing key management in cloud storage using k-out-of-n reliability systems," IEEE Transactions on Cloud Computing, vol. 10, no. 3, pp. 1450–1462, 2022. Available: https://doi.org/10.1109/TCC.2021.3050985
10. A. Chowdhury and D. Koval, Power Distribution System Reliability: Practical Methods and Applications, Hoboken, NJ, USA: John Wiley & Sons, 2011. Available:: https://doi.org/10.1002/9780470454244