Decentralized Ransomware Recovery Network: Enhancing Resilience and Security Through Secret Sharing Schemes

Sijjad Ali[1][a], Jia Wang[1][b], Victor Chung Ming Leung[1][c] and Asad Ali[2][d]

[1]*College of Computer Science and Software Engineering, Shenzhen University, Yuehai Campus, Guangdong, China*

[2]*College of Electronics and information Engineering, Shenzhen University, Yuehai Campus, Guangdong, China*

Keywords: Ransomware, Cybersecurity Defense, Decentralized Ransomware Recovery Network (DRRN), Secret Sharing Schemes, Resilience.

Abstract: Ransomware attacks present multiple threats to individuals such as businesses and organizations, causing data loss, financial stress, and operational interruptions. Traditional measures to mitigate ransomware threats usually include backups and secure applications. However, these countermeasures may not protect against sophisticated attacks. The purpose of this article is to explore a decentralized approach for recovering from multiple ransomware attacks. A decentralized secure approach is employed by the decentralized ransomware recovery network (DRRN) as a platform for sharing data privacy. Backup and restoration of encryption keys on shared domains are performed in the event of a ransomware attack. By paying for ransomware, users can encrypt their files. Additionally, the technical design of the DRRN and its management, as well as ransomware attacks are explored in our studies. A hybrid approach is utilized to evaluate its effectiveness and implications for cybersecurity and data protection. Finally, we assert that our proposed scheme is more secure and effective in the DRRN environment.

1 INTRODUCTION

In recent years, ransomware attacks have increased significantly 68%, posing a serious threat to cybersecurity around the world (Teichmann et al., 2023; Humayun et al., 2021; Ali et al., 2023). There are several characteristics of these cyberattacks that can be summarized as the decryption of sensitive data, the lack of access to legitimate users, as well as the demand for ransom for the key to decryption. Many instances exist where businesses, individuals, and even critical foundations are subjected to severe financial losses, data corruptions, and operational disruptions because of cyber attacks (Kafi and Akter, 2023). A number of traditional methods have been used to prevent the spread of ransomware in recent years. An example of these would be the need for regular backups of data and the use of endpoint security software, as well as incident response protocols (Ilca et al., 2023; Chen et al., 2021). While these measures may provide some protection, they do not succeed in the face of the increasing complexity and targeted nature of contemporary ransomware attacks. This underscores the need for more comprehensive and proactive cybersecurity measures. A proactive approach is crucial against ransomware attacks. We propose state-of-the-art Decentralized Ransomware Recovery Network (DRRN) as a decentralized solution, enhancing recovery processes, reducing attackers' financial incentives, and fortifying data security. DRRN decentralizes control and utilizes secret distribution schemes, ensuring robust and permanent infrastructure for data protection and recovery.

The Decentralized Ransomware Recovery Network (DRRN) utilizes centralized storage approach and use of secret distribution schemes to encrypt very highly sensitive files and keys across networked edge nodes, to making our data secure. In addition, we applied decentralized encryption approach to further secure data and reduce risks of loss or damage during ransomware attacks. The DRRN decentralized storage and encryption keys enhance strength against intrusions, however, secret distribution approach like secret sharing support single-point vulnerabilities. This decrease unauthorized access within the net-

[a] https://orcid.org/0000-0002-9141-8837
[b] https://orcid.org/0000-0002-0861-2496
[c] https://orcid.org/0000-0003-3529-2640
[d] https://orcid.org/0009-0004-5399-0156

Ali, S., Wang, J., Leung, V. and Ali, A.
Decentralized Ransomware Recovery Network: Enhancing Resilience and Security Through Secret Sharing Schemes.
DOI: 10.5220/0012713500003705

In *Proceedings of the 9th International Conference on Internet of Things, Big Data and Security (IoTBDS 2024)*, pages 294-301
ISBN: 978-989-758-699-6; ISSN: 2184-4976

work, enhancing data security against advanced ransomware attacks and minimizing failure risks of network.

In a ransomware attack, the Decentralized Ransomware Recovery Network (DRRN) utilizes distributed shares stored across its nodes to dynamically regenerate the encryption key if it is lost or inaccessible. These shares, fragments of the original key, are reconstructed through secret sharing approach, enabling decryption of the encrypted data. This process allows affected users to regain access to their files without needing to fulfill ransom demands, ensuring fast and reliable recovery. Additionally, the DRRN offers the option to withdraw files from the decryption process if both parties agree, providing flexibility in recovery. By neutralizing the impact of ransomware attacks through decentralized key regeneration, the DRRN removes the financial incentive for attackers and strengthens network security against such threats.

In our proposed work, we perform a deep analysis of the Decentralized Ransomware Recovery Network (DRRN), which maintain its technical architecture, application scope, and practical significance. We explore into decentralization and secret sharing approaches, In addition, emphasizing their function in DRRN defensive solutions against ransomware attacks. Besides, we analyze DRRN efficiency through challenges and simulations, assessing its performance and broader impacts on cybersecurity and data protection. The goal of our analysis is to provide readers with the knowledge to understand DRRN performance and the potential challenges it encounters when combating ransomware attacks in this dynamic cyberspace ecosystem by offering evidence-based insights for informed decision-making.

DRRN is a crucial initiative in ransomware defense establishing proactive and sustainable approaches to prevent breaches and protect critical data. By utilizing a decentralized data distribution approach, it will build a strong defense against ransomware attacks, and the consequent effects will be mitigated to a certain level. By highlighting the crucial role of innovation, this scheme tends to more efficiently deal with recent hacker upgrades and even proactively protect the networks from the threats which may be likely to occur in the future.

2 MAJOR CONTRIBUTIONS

- The DRRN is a decentralized network of nodes all over the network that uses InterPlanetary File System (IPFS) and other decentralized storage methods to offer automatic backups of files that have been decrypted by ransomware. It ensures data integrity and removes the risk of data loss or corruption and single point of failure network.
- The Decentralized Ransomware Recovery Network (DRRN) is divided into multiple contexts by using secret sharing principles, such as Shamar's secret sharing principles, which are distributed across different nodes in the network, so that no single entity contributes significantly to the management of the corruption process as a whole.
- When a victim of ransomware attacks is affected by the Decentralized Ransomware Recovery Network (DRRN), it restores settings in order to relieve them from the financial burden of ransomware attacks, thus allowing affected users to restore their files without making any tact to the attackers.

3 DEFINITION OF SECRET SHARING SCHEME

A secret sharing scheme can be mathematically defined using polynomial interpolation over a finite field (Shamir, 1979). Let's denote;

- S as the secret to be shared.
- n as the total number of participants.
- k as the threshold, i.e., the minimum number of participants required to reconstruct the secret.

A secret sharing scheme involves the following steps;

(1) Polynomial Generation: A polynomial $f(x)$ of degree k_1 is constructed over a finite field $\mathbb{F}$ such that;

$$f(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_1 x + a_0 \quad (1)$$

(2) Secret Allocation: Each participant is assigned a unique x value from the finite field $\mathbb{F}$, and their share s_i is obtained by evaluating the polynomial at that point;

$$s_i = f(x_i) \quad (2)$$

(3) Distribution of Shares: The shares s_i are distributed among the participants.

(4) Reconstruction: To reconstruct the secret S, any subset of k shares can be used with polynomial interpolation. Suppose we have a set of shares $\{(x_1, s_1), (x_2, s_2), \ldots, (x_k, s_k)\}$. We can construct the Lagrange interpolation polynomial $L(x)$ as follows;

$$L(x) = \sum_{i=1}^{k} s_i \cdot l_i(x) \quad (3)$$

Where $l_i(x)$ is the Lagrange basis polynomial given by;

$$l_i(x) = \prod_{j=1, j\neq i}^{k} \frac{x - x_j}{x_i - x_j} \quad (4)$$

The secret S can then be reconstructed as $S = L(0)$.

4 PROPOSED MODEL

The proposed Decentralized Ransomware Recovery Network (DRRN) leverages decentralized storage, a secret sharing scheme, and dynamic key reconfiguration to mitigate ransomware attacks. In the DRRN framework, N decentralized storage nodes are responsible for storing confidential backups of critical files. Employing Shamer's secret sharing scheme with a threshold T, a private message M is divided into shares such that T lower shares are required to reset the key $(T \leq M \leq N)$. The key reset process, which is T-independent, retrieves shares from a subset of nodes post-ransomware attack. Bernoulli's principle is utilized to compute the overall success probability $P_{\text{success}} = 1 - (1-p)^T$, where p represents the probability of success for each share. File recovery, facilitated by the reset key, ensures data retrieval with a success probability $P_{\text{recovery}} = P(K) \times P_{\text{success}}$.

However, the mechanism for detecting ransomware attacks may not be apparent. In the DRRN, all data are encrypted by the user. Consequently, even if an attacker gains access to the encrypted data, their ability to manipulate or utilize it is severely limited. The distributed nature of data storage and the encryption mechanism significantly mitigate the impact of ransomware attacks, ensuring robustness, reducing data loss, and facilitating recovery without compromising data security. This approach effectively minimizes the financial impact on both consumers and organizations. Further details of the proposed model are explained in Figure 1.

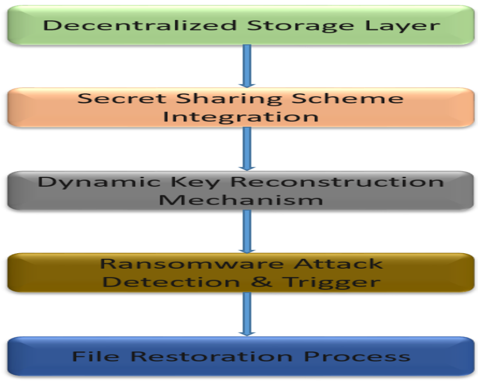

Figure 1: Proposed Model.

5 PROPOSED SCHEME

To enhance reliability and recovery from ransomware attacks, we propose a decentralized DRRN approach that integrates cryptographic principles and mathematical modeling.

5.1 Node Selection Strategy

We selects nodes N for decentralized network backup and secret sharing based on probabilistic values p_i, considering factors like node location, network capacity, and security level. This aims to maximize redundancy and diversity, reducing data loss risk and enhancing network resilience against threats.

5.2 Secret Sharing Process

Shamir's secret distribution method divides a key K into M shares, where T is the minimum number of shares required to reconstruct K. Shares are distributed among nodes based on probabilities p_i. Each share holds no information about the original key until a minimum threshold of shares is gathered, ensuring security against individual node monitoring.

5.3 Probability Modeling for Key Reconstruction

In the context of key reconstruction within Shamir's Secret Sharing scheme, the probability of successfully reconstructing a key, denoted by $P(K)$, is intricately linked to the distribution and accessibility of shares among nodes. Employing binomial distributions $B(M, p)$ proves advantageous in this scenario, with M representing the total number of shares and p delineating the range of access to share edges. As Shamir's Secret Sharing scheme distribute M shares among nodes, the efficacy of edge reconstruction hinges upon the presence of these shares. The binomial distribution adeptly captures this essence by accounting for the minimum number of edges (i.e., total shares M required for successful reconstruction amidst a specified number of accessible shares. This algorithmic approach not only facilitates the estimation of success probability in reconstruction using the available shares but also accommodates potential access restrictions imposed on each share. Consequently, it ensures a robust level of key security by systematically assessing the viability of key reconstruction under various share availability scenarios and access constraints.

Data: M, p, $availableShares$
Result: Probability of successful key reconstruction
Input : Total number of shares M, probability of access to an edge of each share p, number of available shares $availableShares$
Output: Probability of successful key reconstruction

Calculate Probability: $probability \leftarrow 0.0$;
for $k \leftarrow availableShares$ **to** M **do**
  $probability \leftarrow probability + \frac{M!}{k!\cdot(M-k)!} \times p^k \times (1-p)^{M-k}$;
end
return $probability$;

Algorithm 1: Probability Modeling for Key Reconstruction.

5.4 Dynamic Key Reconstruction Mechanism

In this section, the heuristic key construction mechanism is primarily based on the probabilistic distribution of shares. This mechanism prioritizes the return of shares from nodes with a higher probability p_i . After detecting a ransomware attack, the device initiates the release of shares from a fixed number of nodes. This is aimed at joining the threshold T required for key reconstruction. This reconstruction's performance is set according to different factors and considering competing users. This process simplifies and streamlines the initiation of restructuring measures to reduce internal and external risks to shareholders.

5.5 File Restoration Process

The importance of this proposed scheme lies in its ability to optimize the file restoration process, denoted P. This functionality extends beyond just restoration information; it also prevents damages from data modifications or updates. By efficiently restoration data, the system not only restores lost information but also prevents possible changes by adversary to the data. This aspect of operational efficiency is very critical for a security system as it reduces the risk of future attacks that can cause more damage, thereby ensuring revenue and total system resilience. As a result, the ability to restoration data with confidence and accuracy plays a crucial role

Data: p_i, Ransomware attack detection
Result: Reconstructed key
Input : Probability distribution of shares p_i, Ransomware attack detection
Output: Reconstructed key

Key Construction: Initialize priority queue Q;
for *each node i* **do**
  Add node i to Q with priority p_i;
end
Initialize empty list $selectedShares$;
while *not ransomware attack detected* **do**
  Remove node with highest priority from Q;
  Add shares from this node to $selectedShares$;
  if *threshold T reached* **then**
    Break loop;
  end
end
Reconstruction: Reconstruct key using shares from $selectedShares$;

Algorithm 2: Dynamic Key Reconstruction Mechanism.

in the stability and effectiveness of security measures. This strengthens the protection against various threats.

Utilizing probabilistic modeling approach in decentralized ransomware recovery involves statistically assessing the likelihood of successfully recovering encrypted data. This includes factors like the availability and reliability of distributed shares, the chance of each share being retrievable, and the effectiveness of key reconstruction. By evaluating these probabilities, organizations can allocate resources effectively, focusing on areas with the highest chance of successful recovery while minimizing costs. Moreover, this approach enables adaptability to evolving threats and infrastructure changes, refining recovery strategies based on real-world experiences.

6 RESULTS ANALYSIS AND COMPARISON

The data Table 1, presents the different rates of different parameters of the secret distribution scheme, including share size, threshold, success rate, key reconstruction rate, and success rate.

Data: *shares*[], *num_shares*
Result: *key*
Input : Shares array *shares*[], number of shares *num_shares*
Output: Decrypted key *key*

Reconstruct Key: $sum \leftarrow 0$;
$count \leftarrow 0$;
for $i \leftarrow 0$ **to** *num_shares* **do**
  if *shares*[i].*retrieved* **then**
    $sum \leftarrow sum + shares[i].value$;
    $count \leftarrow count + 1$;
  end
end
if $count \geq THRESHOLD$ **then**
  return *sum*;
end
else
  return -1 ; `// Threshold not met`
end

Restore Files: **if** $key \neq -1$ **then**
  print "Files successfully restored using key: *key*";
end
else
  print "Error: Key reconstruction threshold not met";
end

Algorithm 3: Decentralized Ransomware Recovery Algorithm.

6.1 Probability of Key Reconstruction vs. Share Size

Figure 2, shows the relationship between the part size S and the key reconstruction probability $P(K)$ of a secret distribution scheme. In secret sharing schemes, a secret is divided into different parts and distributed among the participants. They can reconstruct the original secret only if a sufficient number of parts, determined by an intermediate parameter called T, are collected. The key reconstruction probability, $P(K)$, predicts the probability of successfully reconstructing a secret in the presence of a specified number of partitions and specified cracks. Mathematically, $P(K)$ is calculated using joint probability, assuming binomial spreading, to calculate the probability of the occurrence of at least T valid segments out of at least S segments. As shown in the figure, the x-axis represents the segment size, which is the number of segments distributed, while the y-axis shows the key reconstruction probability. Each numerical point on the figure represents a specific segment size and key reconstruction probability. In general, we expect that $P(K)$ will show an increasing trend as the segment size increases, indicating the probability of successfully reconstructing the original secret with a larger number of segments, if the old condition fulfills. This figure and mathematical model provide us with a resource in light of the relationship between part size and key reconstruction probability.

The probability for a share size of 5 being larger than for a share size of 7 might seem unreasonable at first glance. However, in certain secret sharing schemes, the relationship between share size and key reconstruction probability can vary based on the specific parameters and assumptions of the scheme. One possible explanation for this phenomenon could be related to the threshold parameter T. If the threshold for successful reconstruction is lower for the share size of 5 compared to 7, it means that fewer shares are required to reconstruct the secret. Consequently, with fewer shares needed, there might be a higher probability of successfully reconstructing the secret with 5 shares compared to 7 shares, even though the share size is smaller. The formula for binomial probability is typically expressed as;

$$P(X \geq T) = \sum_{k=T}^{S} \binom{S}{k} \cdot p^k \cdot (1-p)^{S-k} \tag{5}$$

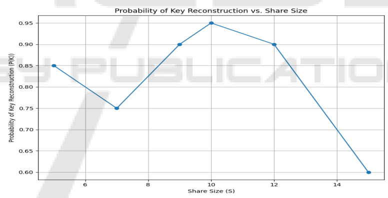

Figure 2: Probability of Key Reconstruction vs. Share Size.

6.2 Probability of Successful Recovery vs. Share Size

Figure 3, shows the relationship between portion size (S) and probability of successful recovery $P(recovery)$ in a secret distribution scheme. In such a scheme, a secret is divided into different parts. The original secret can be recovered if sufficient parts, determined by an intermediate parameter, are collected. Probability of success recovery shows the probability that the secret can be successfully recovered with a given part size and crack. Mathematically, we denote the portion size as S and the probability of success $P(recovery)$ as the probability of success. The relationship between these variables can be modeled on a probabilistic basis. For example, consider the probability of success in production and distribution of each

Table 1: Collected data from experiments.

Share Size (S)	Threshold (T)	Success Probability (p)	Key Reconstruction	Successful Recovery
5	3	0.8	0.85	0.70
7	2	0.6	0.75	0.55
9	4	0.7	0.90	0.80
10	5	0.9	0.95	0.85
12	3	0.8	0.90	0.75
15	6	0.5	0.60	0.45

part. Generally, as the part size increases, the probability of restoration success decreases due to possible causes, such as increasing the number of parts to be taken into account. This is evident in the figure, where the x-axis shows the portion size and the y-axis shows the probability of successful recovery. Each numerical point on the graph represents a specific portion size and its corresponding probability of successful recovery. Analysis of this figure and its mathematical model provides a resource for how the probability of successful recovery changes with different segment sizes.

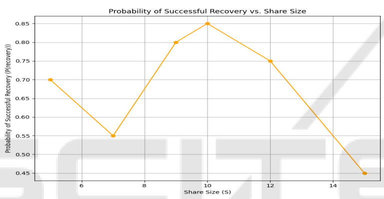

Figure 3: Probability of Successful Recovery vs. Share Size.

6.3 Probability of Key Reconstruction and Successful Recovery vs. Share Size (Combined)

Figure 4, shows a relationship between portion size S and the probability of secret distribution rearrangement and recovery is shown in Figure 4. It is common in such schemes to divide a secret into different parts. An intermediate parameter determines the number of parts needed to recover the original secret. Reordering the keys and recovering the secret is highly likely to be successful, based on the success recovery probabilities. In this case, we assume the partition size and crack size are specified. $P(recovery)$ is the probability of successful recovery, $P(K)$ is the probability of key reordering, and S is the chunk size. Probabilistic realism can be applied to the relationship between these variables. The probability that each part will succeed in production and distribution, for example, is an important consideration. A decrease in key reordering and restoration success is generally associated with increasing part size because of factors, such as the increased number of part geometries. According to the graph, the x-axis represents share size, while the y-axis represents the probability of successful recovery and key reordering. There are numerical points on the graph that represent specific segment sizes and the probability of success for reset and recovery.

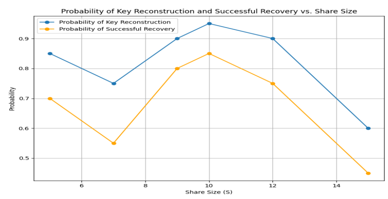

Figure 4: Probability of Key Reconstruction and Successful Recovery vs. Share Size (Combined).

6.4 Comparison

The DRRN model and the SSS method, both introduced in Table 2, are characterized by the robustness and reliability of our proposed scheme, which excels among all the listed research approaches in terms of robustness and reliability. We demonstrate superior resilience and integrity in our scheme, which is different from those used in other articles to address similar issues. It is evident from the high ratings it received in both categories. Our approach is more effective and trustworthy if we use the DRRN model and SSS method.

6.4.1 Robustness Assessment

- The proposed scheme stands out for its high robustness level, utilizing the DRRN model and SSS method, indicating a strong foundation and thorough analysis.
- Notably, it surpasses other studies in robustness, which range from low to medium levels.
- High robustness suggests a well-defined methodology, comprehensive analysis, and reliable findings, providing a solid basis for the proposed scheme's credibility.

6.4.2 Integrity Assessment

- The proposed scheme also demonstrates high integrity, aligning with its high robustness level.

Table 2: Comparison of proposed work.

Authors	Models	Methods	Robustness	Integrity
teichmann et al.(Teichmann et al., 2023)	Economic models	Analysis	Medium	High
fadziso et al.(Fadziso et al., 2023)	Threat modeling frameworks	Overview	Low	Medium
humayun et al.(Humayun et al., 2021)	Ransomware propagation models	Case Studies	low	High
duong et al.(Duong et al., 2023)	Resilience models	Assessment	low	High
kafi et al.(Kafi and Akter, 2023)	Risk assessment frameworks	Case Studies	Medium	High
amoah et al.(Amoah and Steyn, 2023)	Behavioral models	Analysis	Medium	High
ilca et al.(Ilca et al., 2023)	Threat intelligence models	Analysis	High	low
chen et al.(Chen et al., 2021)	Incident response frameworks	Case Studies	Medium	High
bajpai et al.(Bajpai and Enbody, 2023)	Risk management frameworks	Framework	low	High
Our scheme	DRRN model	SSS method	High	High

- High integrity implies trustworthiness, consistency, and transparency in reporting, minimizing potential biases and ensuring data reliability.
- Compared to other studies with varying levels of integrity, the proposed scheme maintains a consistent and trustworthy approach, enhancing its credibility and reliability.

7 SECURITY ANALYSIS

A decentralized cryptographic scheme can be mathematically recovered from ransomware attacks by demonstrating resistance to cyber attacks, ensuring that combined attackers cannot reset the shared secret without the necessary information.

Let's denote:

- n. Total number of participants.
- t. Threshold value (minimum number of shares required to reconstruct the secret).
- S. Set of shares held by colluding adversaries.
- K. Set of honest participants.

A scheme for defense against closure attacks can be mathematically modeled as follows.

7.1 Probability of Successful Collusion Attack

Using these parameters, we calculate the success probability of attackers who optimally configure the secret without the desired crack t. This can be expressed as calculating the key rearranging probability that $|S| \geq t$ given the total number of participants n and the number of slots t. Using combined analysis, we can estimate the probability of success rate, by determining the key of $|S|$ probabilities.

7.2 Threshold Attack

In threshold cryptography, the secret is denoted as S, with derivatives $S_1, S_2, \ldots, S_n$. S is accessible only when realizations meet a fixed threshold t. Subsets below t yield no information about S, as they are statistically independent.

$$P(S \mid S_1, S_2, \ldots, S_{t-1}) = P(S) \tag{6}$$

The equation suggests independence between $S_1, S_2, \ldots, S_n$ and S, ensuring adversaries with gains ¡t gain no info. With knowledge of S entropy and realizations, total probabilities of secret and distributed components can be estimated. Security relies on the inability of combined adversaries to breach the t threshold, ensuring secret protection. Thus, threshold cryptography remains robust against tampering, forming a strong basis for its functionality.

7.3 Entropy Analysis Attack

We explore deeper into the entropy of the secret rearranged by opposing adversaries, which belongs to them. Entropy, denoted $H(S)$, measures the uncertainty or randomness associated with a random variable, in this case, the rearranged secret S'. Considering the entropy of S', denoted as $H(S' \mid S_1, S_2, \ldots, S_k)$, we can determine the extent of invisibility in the arranged secret. Mathematically, this can be expressed as follows:

$$H\left(S' \mid S_1, S_2, \ldots, S_k\right) \leq H\left(S'\right) \tag{7}$$

The fault arises when overlapping shares exist in rearranged secret S'. This constrains the fault range of S', preventing oppressive opponents from breaching absolute secrecy. Mathematical proof shows opposing adversaries lack meaningful info about the secret, requiring access to shares.

8 CONCLUSION AND FUTURE AVENUES

We presented a decentralized ransomware recovery networks utilize mesh networks and secret sharing schemes for heightened security and robustness. By employing layers of security and distributed key management techniques, our solution effectively safeguards sensitive data against ransomware attacks and malicious sharing. Through rigorous mathematical modeling and analytics, we have demonstrated its effectiveness against cyberattacks. In ransomware scenarios, our approach ensures data recovery by decentralizing trust and distributing encryption keys among network nodes.

DRRN future avenues involves enhancing privacy with ICRC technologies, integrating ML and human brain algorithms for ransomware detection, partnering with industries for deployment and assessment. Long-term studies on ransomware risk, adapting DRRN, and legal tasks are included.

ACKNOWLEDGEMENTS

This work was supported in part by the National Key R&D Program of China under Grant 2020YFA0908700, the National Nature Science Foundation of China under Grants 62073225, 62203134, 61972263, 62072315, the Natural Science Foundation of Guangdong Province-Outstanding Youth Program under Grant 2019B151502018, the Natural Science Foundation of Guangdong Province under Grant 2021A1515011153, the Guangdong Pearl River Talent Recruitment Program under Grant 2019ZT08X603, the Guangdong ”Pearl River Talent Plan” under Grant 2019JC01X235, the Shenzhen Science and Technology Innovation Commission under Grant 20200805142159001, JCYJ20220531103401003, JCYJ20210324093808021.

REFERENCES

Ali, S., Wang, J., and Leung, V. C. M. (2023). Defensive strategies against pcc attacks based on ideal (t, n)-secret sharing scheme. *Journal of King Saud University-Computer and Information Sciences*, 35(9):101784.

Amoah, C. and Steyn, D. (2023). Barriers to unethical and corrupt practices avoidance in the construction industry. *International Journal of Building Pathology and Adaptation*, 41(6):85–101.

Bajpai, P. and Enbody, R. (2023). Know thy ransomware response: A detailed framework for devising effective ransomware response strategies. *Digital Threats: Research and Practice*.

Chen, P.-H., Bodak, R., and Gandhi, N. S. (2021). Ransomware recovery and imaging operations: lessons learned and planning considerations. *Journal of Digital Imaging*, 34(3):731–740.

Duong, A. T. B., Hoang, T.-H., Nguyen, T. T. B., Akbari, M., Hoang, T. G., and Truong, H. Q. (2023). Supply chain risk assessment in disruptive times: opportunities and challenges. *Journal of Enterprise Information Management*, 36(5):1372–1401.

Fadziso, T., Thaduri, U., Dekkati, S., Ballamudi, V., and Desamsetti, H. (2023). Evolution of the cyber security threat: an overview of the scale of cyber threat. *Digitalization & Sustainability Review*, 3(1):1–12.

Humayun, M., Jhanjhi, N., Alsayat, A., and Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, 22(1):105–117.

Ilca, L. F., Lucian, O. P., and Balan, T. C. (2023). Enhancing cyber-resilience for small and medium-sized organizations with prescriptive malware analysis, detection and response. *Sensors*, 23(15):6757.

Kafi, M. A. and Akter, N. (2023). Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection. *American Journal of Trade and Policy*, 10(1):15–26.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22(11):612–613.

Teichmann, F., Boticiu, S. R., and Sergi, B. S. (2023). The evolution of ransomware attacks in light of recent cyber threats. how can geopolitical conflicts influence the cyber climate? *International Cybersecurity Law Review*, 4(3):259–280.