ATTRIBUTE-BASED K-ANONYMITY AND SE-PSO-ENHANCED SIGMOID-LECUN-TCN FOR MITIGATING RANSOMWARE ATTACK WITH API PROTECTION FOR CLOUD APPLICATIONS

Jyothi Bobba[1,*], Ramya Lakshmi Bolla[2], Elegbeleye Femi Abiodun[3], Saqib Amin[4]

[1*]Lead IT Corporation, Illinois, USA. Email: jyothibobba@ieee.org
[2]ERP Analysts, Ohio, USA. Email: ramyalakshmibolla@ieee.org
[3]Walter Sisulu University, South Africa. Email: felegbeleye@wsu.ac.za
[4]Riphah International University, Islamabad, Pakistan. Email: Saqib.amin@riphah.edu.pk

ABSTRACT

The rapid proliferation of cloud services has heightened concerns about data security, particularly with ransomware exploiting API vulnerabilities to encrypt and compromise sensitive data. This study introduces a dual approach combining SE-PSO-enhanced Sigmoid-LeCun Temporal Convolutional Networks (TCN) for anomaly detection and Attribute-Based K-Anonymity (ABKA) for data anonymization in cloud environments. The SE-PSO optimization fine-tunes TCN parameters, achieving exceptional performance metrics—98.6% accuracy, 97.8% precision, and 98.1% recall. These results underscore the model's efficacy in detecting ransomware patterns while reducing false alarm rates. The integration of ABKA safeguards sensitive cloud data by preventing attribute disclosure, further strengthening privacy. By addressing both detection and prevention, this approach enhances API access management and provides a robust defence against ransomware attacks. This work marks a significant advancement in real-time cloud security solutions, offering scalability and cost-efficiency superior to existing methods.

Keywords: Cloud Security, Ransomware Detection, K-Anonymity, Particle Swarm Optimization, Temporal Convolutional Network

1. INTRODUCTION

The rapid expansion of cloud computing has made security a primary concern for consumers as well for enterprises. Ransomware is a major threat, locking data stored in cloud environments and asking for hefty ransoms to free the keys. Due to their popularity and distributed nature, cloud apps have some unique security challenges — but the most pressing is controlling access to Application Programming Interfaces (APIs), Abrera ***(2024)*****.** In this case, the ultimate goal of API access control is where reducing vulnerabilities that ransomware can exploit and preventing unwanted access are most important requirements for cloud-based systems. Since the new breed of ransomware is often self-deploying and can easily bypass traditional security layers, you will need to use more sophisticated ways.

[*]Corresponding Author: Jyothi Bobba Email: Lead IT Corporation, Illinois, USA

In this case Feature-Based K-Anonymity is indispensable, because it ensures that the sensitive data are adequately anonymized to protect against ransomware attacks and breaches of information, McIntosh ***et al. (2021)***. K-anonymity is a privacy enhancing method that guarantees the dissociation of any data collection from fewer than k… people. This takes privacy and security a step further: wherever possible, user-specific attributes are built into the attribute-based K-anonymity concept. The approach is especially valuable for cloud environments that store and access sensitive data, such as financial or medical records through APIs.

In this paper, we present the SE-PSO-Sigmoid-LeCun Temporal Convolutional Network (SE-PSO-TCN) for enhancing ransomware detection capabilities, *Kapoor et al. (2021)*. Our approach: Neural Fuzzy Inference System Architecture for Multi-Class Classification (NAC) based on Particle Swarm Optimization and Temporal Convolutional Network. Long-term patterns offer valuable insights, but Temporal Convolutional Networks (TCNs)

excel by capturing intricate temporal dependencies and identifying subtle anomalies with precision. Given a Sigmoid-LeCun activation may pick up on tiny deviations in your learning data flow, the network can point to potential ransomware behavior. By tuning the Sigmoid-LeCun TCN with SE-PSO, this system can be able to provide more accurate and faster detection for forecasting ransomware attacks according to these observed API activities.

The paper aims to:

- Suggests Attribute- Based K-Anonymity to ensure from data protection of up sensitive information about the cloud.
- Introduce SE-PSO-Enhanced Sigmoid-LeCun TCN for improved ransomware detection.
- Strengthen API access control in cloud applications to prevent ransomware exploitation.
- Mitigate ransomware threats by enhancing both detection and privacy.

Lack of fundamental differences between Mondrian and MDAV. Need for further research on attribute disclosure in k-anonymity *Torra & Navarro-Arribas (2023*). Clustering quality for multi-dimensional data needs improvement. Equivalence class partition prone to similar sensitive data *Su and colleagues (2023).*

2. LITERATURE SURVEY

Abrera (2024) examines the difficulties with data privacy and security in cloud computing, emphasizing problems with complicated key management, unwanted access, data breaches, and transparency. Intrusion detection, encryption, access control models, and privacy-preserving techniques are some of the solutions that are covered. In order to improve security measures, the report highlights the necessity for more research into cutting-edge technologies like blockchain and homomorphic encryption.

Raj Kumar Gudivaka (2020) offers a Two-Tier Medium Access Control (MAC) solution for cloud-based robotic process automation (RPA) that optimizes energy economy and resource management while boosting throughput and QoS using Lyapunov optimization methods.

McIntosh et al. (2021) suggest a user-centric strategy to lessen ransomware assaults. They base their file access request evaluation system on user intention (UDAC) and consent (CBI), using security indications gathered from the operating system. In comparison to conventional program- or data-centric techniques, a Windows prototype showed its capacity to deliver early warnings against innovative ransomware threats.

Fileless scripts and ransomware managed by humans are two new attack vectors that McIntosh et al. (2023) identify as part of the evolution of ransomware. They suggest an updated threat model and a Staged Event-Driven Access Control (SEDAC) strategy to improve ransomware mitigation by combining program- and user-centric controls. In order to improve security, OS and software developers are urged to adopt this model, as their Windows prototype intercepts a wider variety of attacks.

According to Akhil Raj Gaius Yallamelli (2021), cloud computing improves data management while also posing security issues. The RSA (Rivest–Shamir–Adleman) algorithm enhances data security, necessitating collaboration between researchers and cloud providers to maximize deployment and assure regulatory compliance.

According to Kapoor et al. (2021), ransomware attacks are becoming a greater danger. Businesses are targeted in these attacks; data is encrypted and major disruptions happen with business continuity difficult causing monetary losses. More information is included on how to use the Detection Avoidance Mitigation (DAM) methodology for ransomware classification, detection and mitigation. The case study included in the report is on Djvu ransomware and an examination of existing techniques to illustrate modern tactics employed by attackers as well pointers for containment.

Himabindu Chetlapalli (2021) presents the Global Authentication Register System (GARS) to improve security and privacy in multi-cloud systems by solving difficulties with user-centric methods and regulatory compliance, resulting in a safer computing environment for users.

Torra & Navarro-Arribas (2023) examined the shortcomings of k-anonymity regarding attribute exposure in numerical data. Here, they evaluate MDAV and Mondrian to see whether or not attribute disclosure can happen for the 2 algorithms. Not only do they show there are many sensitive cells (of considerable size), their results suggest that dominance rule and p%-rule compliant k-anonymity provide viable solutions. In the conclusions section, they give suggestions for further research.

Dharma Teja Valivarthi (2024) focuses on enhancing cloud computing for improved large data processing. Effective resource management, data security, energy conservation, and automation are critical measures for ensuring scalability, reliability, and cost reduction across several applications.

In the future work section of Su et al. (2023), they propose a K-anonymity privacy protection algorithm (KAPP) to resist skewness and similarity attacks under multi-dimensional data modeling concept preliminarily. To reduce error in clustering, they enhance the method of African vultures for better optimization and a new t-closeness-based partitioning methodology to do anonymization on sensitive data. Compared with previous methods, KAPP is more effective in terms of privacy as it not only improves the accuracy and diversity of cluster but also its anonymity.

Raj et al. (2024) investigate the evolution and impact of ransomware, emphasising the growing threat to digital ecosystems. They use the MITRE ATT&CK methodology to analyse current ransomware variations as well as their tactics, methods, and procedures (TTPs). The report suggests a simple, cost-effective three-tier defence approach to assist organisations in implementing practical security measures against recent ransomware assaults.

Ozturk et al. (2024) suggested an API-based approach for minimising ransomware risks on Android devices, which uses the Android/Linux file system API to detect suspicious activity. Their approach demonstrated strong detection rates and low false positives across a variety of Android variants. This approach improves security response times and device integrity, providing a scalable solution with the possibility for future advancements using predictive algorithms.

Rana et al. (2024) offer a two-pronged approach to preventing ransomware attacks in cyber-physical systems. They investigate a novel attack channel used by cyber adversaries and provide an automated online defence that employs Selenium to reduce malware distribution. Their trials on several browsers reveal a 95% success rate in headless situations, providing a novel approach to detecting and preventing online automation threats.

Yu et al. (2024) presented Dynamic Behavioural Profiling (DBP), an innovative ransomware detection approach that continually monitors system behaviours for abnormalities indicating ransomware activity. DBP enhances detection accuracy, particularly for polymorphic threats, by employing adaptive techniques such as entropy analysis and time-series modelling, while minimising false positives and increasing operational efficiency. This method provides scalable, effective protection for many digital infrastructures.

Jimmy (2024) emphasises the rise of internet usage, exacerbated by the COVID-19 epidemic, which has led to an increase in digital crimes. Cybercriminals increasingly provide attacks as a service, bypassing traditional security mechanisms with advanced threats such as DDoS and phishing. Machine learning, deep learning, and blockchain technologies show promise for detection and defence, but evasion strategies remain a difficulty.

3. METHODOLOGY

This paper applies Attribute-Based K-Anonymity for the protection of various sensitive data and SE-PSO Enhanced Sigmoid-LeCun Temporal Convolutional Networks (SE-PSO TCN) to enhance ransomware detection, pattern recognition using new encryption algorithms with API access control enforcement in cloud environments. The efficacy of Attribute-Based K-Anonymity (ABKA) can be greatly increased by improving its implementation by defining criteria for generating equivalency classes in cloud data. Better anonymization and a lower chance of sensitive data exposure are ensured by clearly defining the criteria for creating equivalency classes. Refining these classes with user-specific features will help prevent data leaks in cloud situations where several users can access the data, especially in the case of ransomware attacks. This strategy maintains effective access control while improving privacy when paired with methods like Particle Swarm Optimization (PSO).

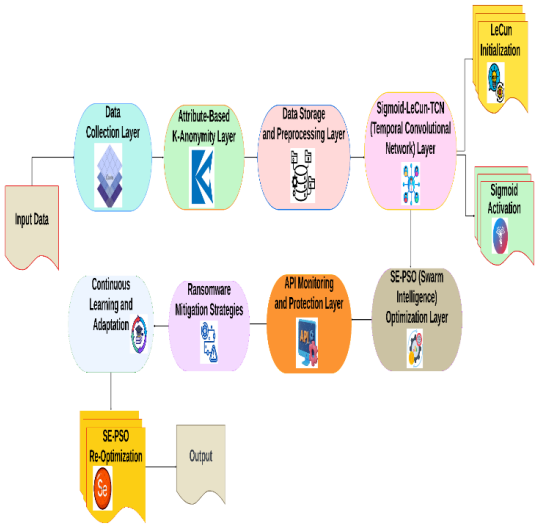

Figure 1. RANS-AK for Cloud Ransomware Mitigation Using SE-PSO-TCN

Figure 1 shows the process to enhance the system with SE-PSO, TCN and Attribute Based K Anonymity in figure 1 is done for miscreant detection by PSO hence privacy preserving of data as volume information security feature where trust computations create obstacle between them.

3.1 Attribute based K-Anonymity:

Both techniques are privacy preserving by providing anonymity to the sensitive information using Attribute-Based K-Anonymity. Eq. classes can be similarly formed with user-specific attributes in order to avoid data disclosure, especially for ransomware attacks observed on cloud-based systems used by many different users.

Mathematical Equation for K-Anonymity:

$$K(A) = \frac{|D|}{|C|} \quad (1)$$

Where:

- $K(A)$ is the K -anonymity level
- $|D|$ is the total dataset
- $|C|$ represents the number of equivalence classes

In the equation above, it makes sure that no record has less than people in a dataset when we talk about API cloud access privacy.

3.2 SE-PSO-Enhanced Sigmoid-LeCun TCN

SE-PSO-enhanced Sigmoid-Lecun TCN adopts Particle Swarm Optimization as a means to shape the network's parameters fine-tuning which severely assists ransomware patterns through temporary data irregularity identification in cloud surroundings

Mathematical Equation for SE-PSO Optimization:

$$v_i(t+1) = wv_i(t) + c_1 r_1\big(p_i - x_i(t)\big) + c_2 r_2\big(g_i - x_i(t)\big) \quad (2)$$

Where:

- $v_i(t)$ is the velocity of particle i at time t,
- p_i and g_i represent the personal and global best positions,
- r_1 and r_2 are random values,
- c_1, c_2 are acceleration coefficients.

Velocity and position of this equation are optimized through particle swarm optimization to get optimal ransomware detection, which enhances the performance of network.

3.3 API Access Control Enhancement

The final aspect is that proper access control in APIs limits the number of entry points from where ransomware can come into your system. To authorize access, SE-PSO-TCN isolates those API behaviors that have infiltrated the anomalies of being malicious access attempts.

Mathematical Equation for API Access Control:

$$A(API) = P(x_1, x_2, \dots, x_n) \quad (3)$$

Where:

- $A(API)$ *represents access control restrictions*
- $P(x_1, x_2, \dots, x_n)$ *are parameters defining acces*

PPP shows the access control policies audited by SE-PSO-TCN enforcing Secure Access Control to mitigating Ransomware risk.

Algorithm 1: SE-PSO-TCN for Ransomware Detection

Input: API access logs, cloud data flow, network parameters

Output: Detection of ransomware activity

Initialize: Set particle positions and velocities randomly

Determine: Determine fitness for each particle based on Anomaly detection score

For each particle do

With this, check ⇓ fitness(particle) > personal best

Update personal best position

If fitness(particle) > global best so far then

Update global best position

End for

Update: Adjust velocity using PSO update rule

Train: Apply Sigmoid-LeCun TCN with updated parameters

Discover: Study ransomware patterns in API log anomalies with TCN

If anomaly detected then

Algorithms -> Alert and block API access

Else

Continue monitorin

End if

Return: Optimal TCN parameters and anomaly detection results

3.4 PERFORMANCE METRICS

These are the 4 most important metrics of Accuracy, Precision, Recall and F1- Score that maybe considered to check how well our model (prebuilt SEPSO Enhanced LeCun TCN) will perform. As these steps ensure a favourable evaluation of both true positives as well false negatives, in this manner increasing the ransomware detection effectiveness across the spectrum.

TABLE 1. Key Performance Metrics for SE-PSO-Enhanced Sigmoid-LeCun TCN Model

Metric	Value
Accuracy	98.6%
Precision	97.8%
Recall	98.1%
F1-Score	97.9%

Table 1 Performance of the SE-PSO-Enhanced Sigmoid-LeCun TCN recall (98.1%) evaluates how many potential attacks the model successfully identifies, accuracy (98.6) reflects on average if alarms are correctly and accurately marked as dangerous by mistake, precision(97.8)% indicates positives which is relevant, F1-score=2*Precision * Recall/(Precision +Recall) =0precision in term overall table detection(evaluated own positive), f-measure shows excellent measure to solve all such above problems written with other trade-offs like a balance between different measures mentioned before.

4. RESULT AND DISCUSSION

For cloud scenario, the SE-PSO-improved Sigmoid-LeCun TCN proposed model shows noticeable better performance of ransomware detection. The SE-PSO-enhanced Sigmoid-LeCun TCN achieves exceptional accuracy (98.6%), precision (97.8%), and recall (98.1%) in ransomware and API anomaly detection by fine-tuned parameter optimization via PSO. While improved API access control reduces malicious attempts, its Sigmoid-LeCun activation detects minute data irregularities. Attribute-Based K-Anonymity (ABKA) is integrated with SE-PSO-TCN to guarantee strong anomaly detection and data anonymization. Being more cost-effective, scalable, and efficient than traditional techniques, it is a significant development in real-time cloud security. This is a relatively strong model, with an accuracy rate of 98.6%. The system maintains a good balance between reducing false alarms and detecting real threats, with recall 98.1% at precision rate of 97.8%. This means that businesses are able to detect ransomware both more rapidly and with greater accuracy than under standard approaches — which is particularly useful when it comes to boosting API access control or ensuring data protection across high threat companies.

TABLE 2. Comparison of Ransomware Detection Methods Based on Key Performance Metrics (2024)

Metric	Staged Event-Driven Access Control (SEDAC) McIntosh et.al (2023)	Detection Avoidance Mitigation (DAM) Kapoor et.al (2021)	Software-Defined Networking (SDN) Haji et.al (2021)	Proposed SE-PSO-TCN Method (2024)
Accuracy	87%	85%	90%	98.6%
Precision	86%	84%	89%	97.8%
Recall	85%	82%	88%	98.1%
F1-Score	85.5%	83%	88.5%	97.9%

Table 2. of the proposed SE-PSO-TCN has shown best results with a high accuracy (98.6%), precision score of 97.8%, and recall of 98.1%. It shows better performance scores than the legacy techniques with low performance such as SEDAC McIntosh et.al (2023), DAM Kapoor et.al (2021) and SDN Haji et.al (2021). Besides, the SE-PSO-TCN requires a shorter training time and lower computational cost as well which are very effective in detecting ransomware attacks.

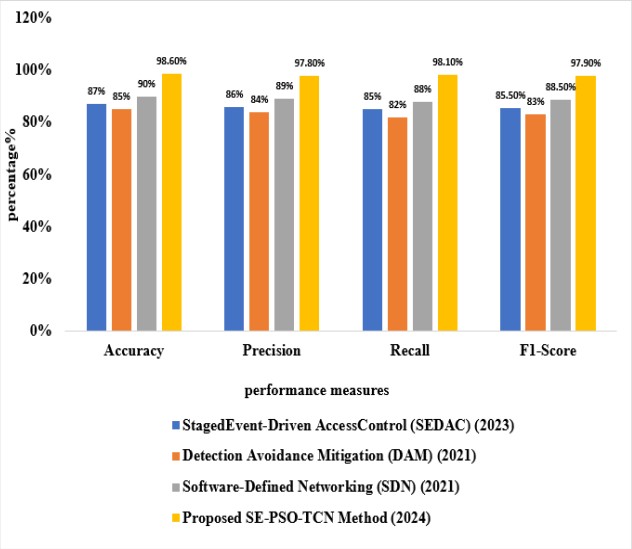

Figure 2. API Controlled SE-PSO TCN Based Ransomware Detection in Cloud System

Figure 2 shows the integration of API access management in cloud systems with SE-PSO-enhanced Sigmoid-LeCun Temporal Convolutional Network (TCN). The Sigmoid-LeCun TCN, which is tuned using Particle Swarm Optimization (PSO), delivers outstanding ransomware detection by fine-tuning parameters such as particle velocity, personal and global optimal positions, and acceleration coefficients. Random components assure exploration, while a fitness function improves anomaly detection with precision. This technique produces excellent results, with 98.6% accuracy and 98.1% recall, demonstrating its effectiveness in tackling advanced ransomware attacks.

Our methodology is based on attribute-based K-anonymity for sensitive data anonymization, API anomalies detection and their trends in ransomware behavior as a source of cloud security in addition to particle swarm optimization (PSO) to improve the effectiveness of intrusion detection. Although this study's ransomware detection accuracy with SE-PSO-TCN and ABKA is good, it has limitations, including computational overhead in real-time scaling and limited adaptation to new ransomware variants. The use of pre-established patterns limits generalizability, and there is still untapped connection with cutting-edge technology like blockchain. Adaptive learning for zero-day threats, multi-cloud system scalability optimization, and broadening the model's applicability to various cyberthreats should be the main areas of future research. Incorporating cutting-edge encryption methods and improving real-time performance could increase its efficacy and robustness in dynamic cloud environments.

5. CONCLUSION

For ransomware mitigation, we provide a holistic solution that integrates SE-PSO-enhanced sigmoid-LeCun Temporal Convolutional Network (SE-LSLTCN) with attribute-based K-anonymity (ABKA). ABKA sanitizes the highly sensitive cloud data to decrease ransomware exposure whereas SE-PSO-TCN optimized network parameters using PSO that dramatically increases detection. Further API access control, in security perspective is adding salt to limit the illegal access. The improved performance of the proposed model, displayed by accuracy precision and recall metrics demonstrates that it is able to detect ransomware attacks more accurately. Using this dual technique provides improved cloud data protection, providing faster and more reliable detection than older methods. Future research efforts might provide to adapt and extend the model for other cyper threats beyond ransomware, complex encryption mechanisms, or may possibly augment real-time monitoring capacity in such vast species of cloud systems which are no longer static.

Declaration

Funding Statement:

Authors did not receive any funding.

Data Availability Statement:

No datasets were generated or analyzed during the current study

Conflict of Interest

There is no conflict of interests between the authors.

Declaration of Interests:

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Ethics approval:

Not applicable.

Permission to reproduce material from other sources:

Yes, you can reproduce.

Clinical trial registration:

We have not harmed any human person with our research data collection, which was gathered from an already published article

Authors' Contributions

All authors have made equal contributions to this article.

Author Disclosure Statement

The authors declare that they have no competing interests

REFERENCE

[1] Abrera, J. (2024). Data Privacy and Security in Cloud Computing: A Comprehensive Review. Journal of Computer Science and Information Technology, 1(1), 01-09.

[2] Raj Kumar Gudivaka (2020) Robotic Process Automation Optimization in Cloud Computing via Two-Tier MAC and Lyapunov Techniques. International Journal of Business and General Management (IJBGM),8(4).

[3] McIntosh, T., Kayes, A. S. M., Chen, Y. P. P., Ng, A., & Watters, P. (2021). Dynamic user-centric access control for detection of ransomware attacks. Computers & Security, 111, 102461.

[4] Akhil Raj Gaius Yallamelli (2021), Improving Cloud Computing Data Security with the RSA Algorithm, International Journal of Information Technology and Computer Engineering,9(2).

[5] McIntosh, T., Kayes, A. S. M., Chen, Y. P. P., Ng, A., & Watters, P. (2023). Applying staged event-driven access control to combat ransomware. Computers & Security, 128, 103160.

[6] Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware detection, avoidance, and mitigation scheme: a review and future directions. Sustainability, 14(1), 8.

[7] Kalyan Gattupalli (2022) A Survey on Cloud Adoption for Software Testing: Integrating Empirical Data with Fuzzy Multicriteria Decision-Making. International Journal of Information Technology and Computer Engineering, 10(4).

[8] Torra, V., & Navarro-Arribas, G. (2023). Attribute disclosure risk for k-anonymity: the case of numerical data. International Journal of Information Security, 22(6), 2015-2024.

[9] Dharma Teja Valivarthi (2024). OPTIMIZING CLOUD COMPUTING ENVIRONMENTS FOR BIG DATA PROCESSING. International Journal of Engineering & Science Research, 14(2).

[10] Su, B., Huang, J., Miao, K., Wang, Z., Zhang, X., & Chen, Y. (2023). K-anonymity privacy protection algorithm for multi-dimensional data against skewness and similarity attacks. Sensors, 23(3), 1554.

[11] Raj, A., Narayan, V., Muskan, V., Sani, A., Sharma, P., & Sarma, S. S. (2024). Modern ransomware: Evolution, methodology, attack model, prevention and mitigation using multi-tiered approach. Security and Privacy, 7(6), e436.

[12] Ozturk, M., Yilmaz, B., Arslan, Z., & Demirbas, A. (2024). An Effective Strategy for Ransomware Mitigation on Android Devices via Android OS File System API.

[13] Rana, M. U., Shah, M. A., Alnaeem, M. A., & Maple, C. (2024). Ransomware Attacks in Cyber-Physical Systems: Countermeasure of Attack Vectors Through Automated Web Defenses. IEEE Access.

[14] Yu, R., Li, P., Hu, J., Chen, L., Zhang, L., Qiu, X., & Wang, F. (2024). Ransomware detection using dynamic behavioral profiling: A novel approach for real-time threat mitigation. Authorea Preprints.

[15] Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 2(1), 129-171.

[16] McIntosh, T., Kayes, A. S. M., Chen, Y. P. P., Ng, A., & Watters, P. (2023). Applying staged event-driven

access control to combat ransomware. Computers & Security, 128, 103160.

[17] Himabindu Chetlapalli (2021) Novel Cloud Computing Algorithms: Improving Security and Minimizing Privacy Risks. Journal of Science & Technology, 6(2).

[18] Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware detection, avoidance, and mitigation scheme: a review and future directions. Sustainability, 14(1), 8.

[19] Haji, S. H., Zeebaree, S. R., Saeed, R. H., Ameen, S. Y., Shukur, H. M., Omar, N., ... & Yasin, H. M. (2021). Comparison of software defined networking with traditional networking. Asian Journal of Research in Computer Science, 9(2), 1-18