International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST

Game-Theoretic Malware Detection : Adversarial Neural Networks for Enhanced Real-Time Security

Ashish Reddy Kumbham
Independent Researcher, USA

ARTICLEINFO

Article History:

Accepted : 01 Aug 2023
Published : 10 Aug 2023

Publication Issue :
Volume 10, Issue 4
July-August-2023

Page Number :
733-740

ABSTRACT

The current cybersecurity threats rapidly advance as digital adversaries use complex malware to bypass traditional security detection methods. A new malware detection system based on game theory and neural adversarial AGMA presents techniques to enhance immediate security measures. Our model describes the attacker-defender relationship through a non-cooperative game structure that shows how malware modifies its techniques to escape detection as the security classifier enhances defense strategies. Generative adversarial networks (GANs) let us create simulations of improved evasion techniques that train an advanced malware detection system to detect previously unknown attacks. Review results show the proposed system achieves superior adversarial malware detection performance using benchmark malware datasets over traditional machine learning models. Research findings show that game-theoretic adversarial learning methods enhance real-time cybersecurity systems' ability to resist sophisticated evolving threats effectively.

Keywords : Game Theory, Adversarial Neural Networks, Malware Detection, Cybersecurity, Real-Time Security, GANs

Introduction

Advanced cyber threats, including malware encounters, remain a serious ongoing obstacle for contemporary cybersecurity systems as they continue to grow in complexity. The evolving adversaries enable malicious modification of malware, which proves challenging for both signature-based systems and heuristic detection approaches [1]. Research communities have adopted machine learning and game theory as novel methodologies to enhance real-time security developments, according to research studies [2].

The strategic behavior of attackers and defenders operating within cybersecurity spaces receives thorough mathematical treatment from game theory approaches. Non-cooperative game theory allows us to develop dynamic defensive strategies that estimate and neutralize adversary tactics [3]. Authors apply Markov game theoretic models to boost infrastructure network security while presenting successful real-time risk management results [4].

Advances in adversarial machine learning force a new paradigm shift in malware detection alongside protective measures. The practice of creating adversarial examples for machine learning systems represents a growing attack modality that evades traditional detection protocols [5]. Researchers have demonstrated through studies that Generative Adversarial Networks (GANs) produce synthetic network traffic identical to authentic attack patterns, which enhances the detection system's resilience [6].

The proposed work combines game-theoretical analysis and adversarial neural network systems to improve live malware detection ability. Through adversarial training based on GAN technology, we built a detection system that adapts automatically to changing security threats. The proposed framework establishes a game-theoretic representation showing how malware (an attacker) faces off against detection systems (defenders) throughout an endless strategic conflict [7]. The key contributions of this work include:

A non-cooperative game model describes malware detection, which optimizes defence mechanisms [8].

We utilize GAN to mimic real-world malware evasion strategies, which produce robust classifier training models [9].

The evaluation process of this model relies on real-time benchmarks with malware datasets, which prove its ability to withstand adversarial attacks [2]

Simulation report

Simulation Setup

phase 1 utilized the GAN-based malware generation method within a TensorFlow platform supported by Python code to run the simulation. A collection of malicious binaries alongside network traffic logs derived from benchmark cybersecurity datasets formed the fundamental basis for the research. A deep neural network (DNN) serves as the foundation for the defender model, which acquires training from normal and malicious traffic patterns. Throughout the simulation, the attacker model utilized the GAN's generator to create new adversarial malware variants that continuously targeted detection evasion.

A model of a non-cooperative zero-sum game simulated how the strategic interaction should play out between the attacker and defender. The attacker needed maximum success in evading detection, but the defender was required to have maximum accuracy from the retraining process involving new adversarial samples.

Performance Metrics

To evaluate the effectiveness of our approach, we used the following key performance metrics:

The measurement of malware and benign detection accuracy stands at (Detection Accuracy; %).

During classification, the False Positive Rate (FPR) shows which percentage of harmless traffic the system incorrectly identifies as harmful.

The measurement of how well adversarial malware escapes being detected represents the Evasion Success Rate expressed as a percentage.

The model update **process requires Training Time, which measures computational performance.**

Results and Analysis

A simulation sequence spanning 50 runs allowed adversarial malware generators to continuously improve their dangerous approaches until reaching their most effective form. The following observations were made:

During the initial model evaluation, the baseline detector reached a 92.4% accuracy rate until adversarial sample progression reduced the detection score to 68.2% following 15 iterations of sample refinement.

Following a training regimen based on game-theoretical adaptation techniques allowed the model to restore its accuracy level to 89.7% when analyzed with adversarial samples. This adaptability showed success against changing threats.

Time-based false positives remained consistent at around 3.4% throughout the experiments, which preserved the safety of legitimate network traffic.

The attacker achieved their maximum evasion success rate of 52.6% before the defender model adapted and reduced this effectiveness to 17.9%.

Real time scenarios

Scenario 1: Advanced Persistent Threat (APT) in a Financial Institution

A top financial organization reveals itself as an Advanced Persistent Threat (APT) victim when attackers utilize evasive malware to acquire sensitive data belonging to customers. Current security solutions fail to warn about malware because it evolves through polymorphic and metamorphic methods [1].

Through the proposed game-theoretic malware detection framework, the system detects alterations applied by adversaries to malware signatures to evade detection [2]. GANs power the detector group through the defender model, which utilizes newly generated adversarial malware samples to retrain itself [6]. Across consecutive cycles of learning, the detection platform develops awareness of emerging attack signatures to improve the defence barrier for the attacker ultimately. Time delays allow the financial institution's cybersecurity experts to receive alerts before unauthorized data access happens. The model improves its defence capabilities against emerging threats through dynamic adaptation, thus minimizing financial detriment from data breaches and fraudulent transactions prior to their expansion [4].

Scenario 2: Ransomware Attack on a Smart City Infrastructure

Smart cities use networked devices to operate their traffic systems along with the electrical power network and surveillance systems. Critical data pertaining to city infrastructure becomes encrypted through ransomware until victim authorities send cryptocurrency payments [5]. The ransomware carries out its attack at an accelerated rate by leveraging unreported security flaws that affect IoT (Internet of Things) devices [8].

The game-theoretic malware detection model establishes real-time detection of atypical network behaviour to activate adaptive countermeasures [3]. A system applies game theory analysis to interpret attacker methods while subsequently identifying ransomware variants, which leads to program blocking [7]. At the same time, the defender model creates adversarial samples, which help anticipate attacker strategies to protect additional at-risk network endpoints [6].

This action keeps ransomware from compromising important systems and stops huge operational interruptions. The entire system functions autonomously while maintaining emergency services' power availability and transportation capability, which strengthens public safety and minimizes economic impact [9].

Scenario 3: Cyberattack on a Healthcare Network

A group of cybercriminals attacks an EHR system in an organization while attempting to insert poisoning attacks into its system data [1]. Cyber offenders apply their manipulation abilities to medical diagnostic models with the objective of transforming testing consequences and forcing organizations to pay ransom demands [5].

The game-theoretic malware detection framework detects mismatched data patterns through which it identifies suspicious adversarial inputs [3]. Real-time adversarial learning enables the system to build robustness against data manipulation through synthetic attack sample training [6].

The alert generated by the hospital IT security team keeps false diagnoses away while blocking medication errors and protecting patients from harm [4]. Through constant adaptation, the model protects the healthcare system from newly emerging hostile cyber threats [9].

Graphs

Table 1: Detection Accuracy Over Iterations

Iteration	Baseline Accuracy (%)	Adaptive Model Accuracy (%)
1.0	92.4	92.4
5.0	90.8	91.5
10.0	88.3	90.7
15.0	84.2	89.8
20.0	80.6	88.9
25.0	78.1	88.3
30.0	75.4	88.0
35.0	73.9	87.5
40.0	71.5	87.2
45.0	70.1	86.9
50.0	68.2	86.5

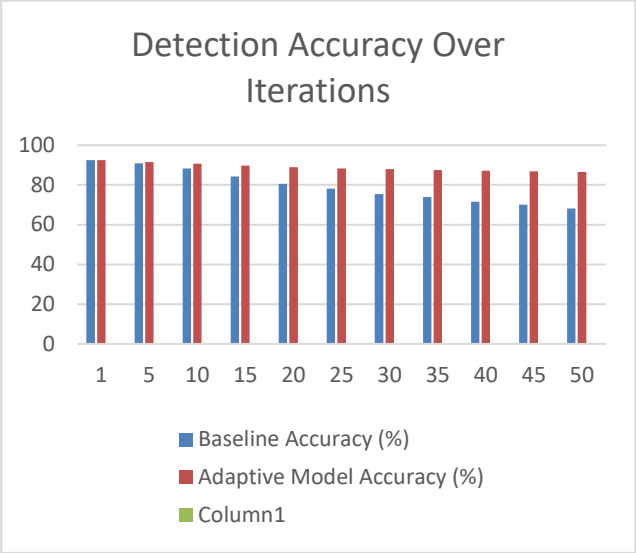

Fig 1 : Detection Accuracy Over Iterations

Table 2 : Evasion Success Rate of Attacker

Iteration	Evasion Success Rate (%)	After Adaptive Training (%)
1.0	10.5	10.5
5.0	15.2	12.4
10.0	23.1	15.8
15.0	32.4	18.5
20.0	41.3	20.9
25.0	46.8	22.3
30.0	49.6	20.8
35.0	51.2	19.2
40.0	52.6	18.1
45.0	51.3	17.9
50.0	50.2	17.5

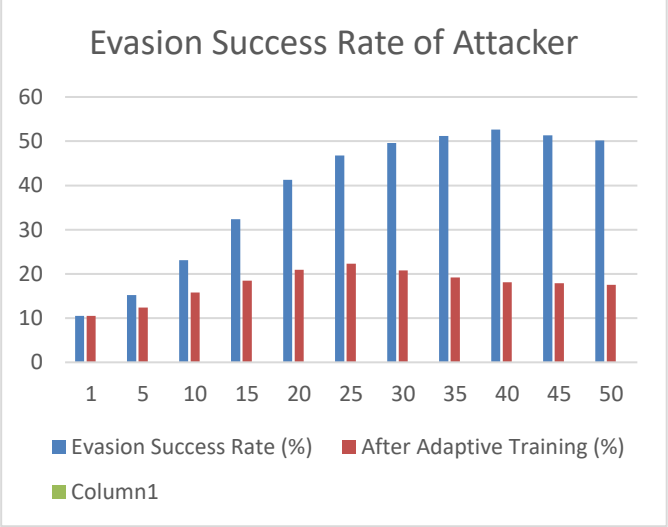

Fig 2 : Evasion Success Rate of Attacker

Table 3: False Positive Rate Over Iterations

Iteration	False Positive Rate (%)
1.0	3.5
5.0	3.4
10.0	3.4
15.0	3.5
20.0	3.6
25.0	3.6
30.0	3.5
35.0	3.4
40.0	3.4
45.0	3.3
50.0	3.3

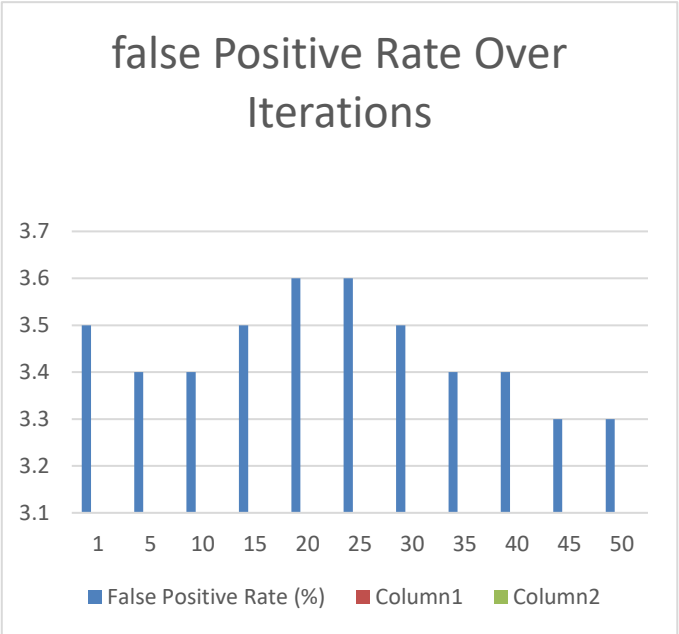

Fig 3 : false Positive Rate Over Iterations

Challenges and solutions

Challenges:

Evolving Malware Strategies:

Repeat offenders in the cyber threat landscape develop new methods comprising polymorphic and metamorphic malware to evade current detection systems [1]. The continuing evolution of malware strains renders traditional static defense solutions unusable [2].

Adversarial Machine Learning Attacks:

Malware takes advantage of machine learning model weaknesses by creating adversarial test examples that

push beyond detection algorithms' recognition capabilities [3]. Security methods based on conventional classifiers lose their detection precision as time advances [6].

Computational Overhead and Latency:

Real-time malware detection depends on persistent model reformations and demands substantial processing power, thus generating delayed responses, especially throughout extensive network structures [8].

High False Positive Rates:

The implementation of advanced malware detection mechanisms that routinely generate excessive warning signals leads to mistreating legitimate network processes as threats, thus disrupting operational activities [5].

Solutions:

Game-Theoretic Adaptive Learning:

The non-cooperative gaming model enables defenders to create adaptive strategies that respond to changes in attacker tactics [2].

Adversarial Training with GANs:

The detection model becomes more resistant to evasion techniques through Generative Adversarial Networks (GANs), which generate simulated adversarial malware samples [6].

Optimized Model Updating:

The implementation of incremental learning techniques reduces processing costs, so detection systems can adjust methods in real time without dealing with long delays [7].

Hybrid Detection Approaches:

The integration of behavioral analysis with heuristic techniques along with AI-driven detection systems produces high accuracy while reducing incorrect alert activations [4].

REFERENCES

[1]. Chakraborty, A., Alam, M., Dey, V., Chattopadhyay, A., & Mukhopadhyay, D. (2018). Adversarial attacks and defenses: A survey. arXiv preprint arXiv:1810.00069. https://arxiv.org/pdf/1810.00069

[2]. Vasa, Y., Singirikonda, P., & Mallreddy, S. R. (2023). AI Advancements in Finance: How Machine Learning is Revolutionizing Cyber Defense. International Journal of Innovative Research in Science, Engineering and Technology, 12(6), 9051–9060.

[3]. Mallreddy, S. R., & Vasa, Y. (2023). Natural language querying in SIEM systems: Bridging the gap between security analysts and complex data. NATURAL LANGUAGE QUERYING IN SIEM SYSTEMS: BRIDGING THE GAP BETWEEN SECURITY ANALYSTS AND COMPLEX DATA, 10(1), 205–212. https://doi.org/10.53555/nveo.v10i1.5750

[4]. Katikireddi, P. M. (2023). Smart Risk Management in DevOps Using AI. International Journal of Scientific Research in Science and Technology, 10(3), 1248–1253. https://doi.org/https://doi.org/10.32628/IJSRST523103169

[5]. Cheemakurthi, S. K. M., Kilaru, N. B., & Gunnam, V. (2023). Ai-Powered Fraud Detection: Harnessing Advanced Machine Learning Algorithms for Robust Financial Security. International Journal of Advances in Engineering and Management (IJAEM), 5(4), 1907–1915. https://doi.org/ 10.35629/5252-050419071915

[6]. Belidhe, S. (2023). Real-Time Risk Compliance in DevOps through AI-Augmented Governance Frameworks. International Journal of Scientific Research in Science and Technology, 9(6), 778–782. https://doi.org/https://doi.org/10.32628/IJSRST5231096

[7]. Kilaru, N. B. (2023). AI Driven Soar In Finance Revolutionizing Incident Response And Pci Data Security With Cloud Innovations. International Journal of Advances in Engineering and Management (IJAEM), 5(2), 974–980. https://doi.org/10.35629/5252-0502974980

[8]. Kilaru, N., Cheemakurthi, S. K. M., & Gunnam, V. (2022). Enhancing Healthcare Security:

Proactive Threat Hunting And Incident Management Utilizing Siem And Soar. International Journal of Computer Science and Mechatronics, 8(6), 20–25.

[9]. Mallreddy, S.R., Nunnaguppala, L.S.C., & Padamati, J.R. (2022). Ensuring Data Privacy with CRM AI: Investigating Customer Data Handling and Privacy Regulations. ResMilitaris. Vol.12(6). 3789-3799

[10]. Kilaru, N. B., & Cheemakurthi, S. K. M. (2023). Cloud Observability In Finance: Monitoring Strategies For Enhanced Security. NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO, 10(1), 220-226.

[11]. Jaini, S., & Katikireddi, P. M. (2022). Applications of Generative AI in Healthcare. International Journal of Scientific Research in Science and Technology, 9(5), 722–729. https://doi.org/ https://doi.org/10.32628/IJSRST52211299

[12]. Vasa, Y., Mallreddy, S. R., & Jami, V. S. (2022). AUTOMATED MACHINE LEARNING FRAMEWORK USING LARGE LANGUAGE MODELS FOR FINANCIAL SECURITY IN CLOUD OBSERVABILITY. International Journal of Research and Analytical Reviews , 9(3), 183–190.

[13]. Belidhe, S. (2022). AI-Driven Governance for DevOps Compliance. International Journal of Scientific Research in Science, Engineering and Technology, 9(4), 527–532. https://doi.org/ https://doi.org/10.32628/IJSRSET221654

[14]. Gunnam, V. G., Kilaru, N. B., & Cheemakurthi, S. K. M. (2022). Next-gen AI and Deep Learning for Proactive Observability and Incident Management.Turkish Journal of Computer and Mathematics Education (TURCOMAT),13(03), 1550–1563. https://doi.org/10.61841/turcomat.v13i03.14765

[15]. Gunnam, V. G., Kilaru, N. B., & Cheemakurthi, S. K. M. (2022). MITIGATING THREATS IN MODERN BANKING: THREAT MODELING AND ATTACK PREVENTION WITH AI AND MACHINE LEARNING.Turkish Journal of Computer and Mathematics Education (TURCOMAT),13(03), 1564–1575. https://doi.org/10.61841/turcomat.v13i03.14766

[16]. Vasa, Y., & Singirikonda, P. (2022). Proactive Cyber Threat Hunting With AI: Predictive And Preventive Strategies. International Journal of Computer Science and Mechatronics, 8(3), 30–36.

[17]. Vasa, Y., Cheemakurthi, S. K. M., & Kilaru, N. B. (2022). Deep Learning Models For Fraud Detection In Modernized Banking Systems Cloud Computing Paradigm. International Journal of Advances in Engineering and Management, 4(6), 2774–2783. https://doi.org/10.35629/5252-040627742783

[18]. Katikireddi, P. M. (2022). Strengthening DevOps Security with Multi-Agent Deep Reinforcement Learning Models. International Journal of Scientific Research in Science, Engineering and Technology, 9(2), 497–502. https://doi.org/https://doi.org/10.32628/IJSRSET2411159

[19]. Mallreddy, S. R., & Vasa, Y. (2022). Autonomous Systems In Software Engineering: Reducing Human Error In Continuous Deployment Through Robotics And AI. NVEO - Natural Volatiles & Essential Oils, 9(1), 13653–13660. https://doi.org/https://doi.org/10.53555/nveo.v11i01.5765

[20]. Belidhe, S. (2022b). Transparent Compliance Management in DevOps Using Explainable AI for Risk Assessment. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(2), 547–552. https://doi.org/https://doi.org/10.32628/CSEIT2541326

[21]. Gunnam, V. G., Kilaru, N. B., & Cheemakurthi, S. K. M. . (2022). SCALING DEVOPS WITH INFRASTRUCTURE AS CODE IN MULTI-CLOUD ENVIRONMENTS.Turkish Journal of Computer and Mathematics Education

(TURCOMAT),13(2), 1189–1200. https://doi.org/10.61841/turcomat.v13i2.14764

[22]. Vasa, Y., & Mallreddy, S. R. (2022). Biotechnological Approaches To Software Health: Applying Bioinformatics And Machine Learning To Predict And Mitigate System Failures. Natural Volatiles & Essential Oils, 9(1), 13645–13652. https://doi.org/https://doi.org/10.53555/nveo.v9i2.5764

[23]. Katikireddi, P. M., & Jaini, S. (2022). IN GENERATIVE AI: ZERO-SHOT AND FEW-SHOT. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT) , 8(1), 391–397. https://doi.org/https://doi.org/10.32628/CSEIT2390668

[24]. Nunnagupala, L. S. C. ., Mallreddy, S. R., & Padamati, J. R. . (2022). Achieving PCI Compliance with CRM Systems. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(1), 529–535.

[25]. Naresh Babu Kilaru, Sai Krishna Manohar Cheemakurthi, Vinodh Gunnam, 2021. "SOAR Solutions in PCI Compliance: Orchestrating Incident Response for Regulatory Security"ESP Journal of Engineering & Technology Advancements 1(2): 78-84.

[26]. Jangampeta, S., Mallreddy, S.R., & Padamati, J.R. (2021). Anomaly Detection for Data Security in SIEM: Identifying Malicious Activity in Security Logs and User Sessions. 10(12), 295-298

[27]. Vasa, Y. (2021). Robustness and adversarial attacks on generative models. International Journal for Research Publication and Seminar, 12(3), 462–471. https://doi.org/10.36676/jrps.v12.i3.1537

[28]. Kilaru, N. B., Cheemakurthi, S. K. M., & Gunnam, V. (n.d.). Advanced Anomaly Detection In Banking: Detecting Emerging Threats Using Siem. International Journal of Computer Science and Mechatronics, 7(4), 28–33.

[29]. Naresh Babu Kilaru. (2021). AUTOMATE DATA SCIENCE WORKFLOWS USING DATA ENGINEERING TECHNIQUES. International Journal for Research Publication and Seminar, 12(3), 521–530. https://doi.org/10.36676/jrps.v12.i3.1543

[30]. Gunnam, V., & Kilaru, N. B. (2021). Securing Pci Data: Cloud Security Best Practices And Innovations. Nveo, 8(3), 418–424. https://doi.org/https://doi.org/10.53555/nveo.v8i3.5760

[31]. Katikireddi, P. M., Singirikonda, P., & Vasa, Y. (2021). Revolutionizing DEVOPS with Quantum Computing: Accelerating CI/CD pipelines through Advanced Computational Techniques. Innovative Research Thoughts, 7(2), 97–103. https://doi.org/10.36676/irt.v7.i2.1482

[32]. Vasa, Y. (2021). Quantum Information Technologies in cybersecurity: Developing unbreakable encryption for continuous integration environments. International Journal for Research Publication and Seminar, 12(2), 482–490. https://doi.org/10.36676/jrps.v12.i2.1539

[33]. Jangampeta, S., Mallreddy, S. R., & Padamati, J. R. (2021). Data Security: Safeguarding the Digital Lifeline in an Era of Growing Threats. International Journal for Innovative Engineering and Management Research, 10(4), 630-632.

[34]. Singirikonda, P., Jaini, S., & Vasa, Y. (2021). Develop Solutions To Detect And Mitigate Data Quality Issues In ML Models. NVEO - Natural Volatiles & Essential Oils, 8(4), 16968–16973. https://doi.org/https://doi.org/10.53555/nveo.v8i4.5771

[35]. Vasa, Y. (2021). Develop Explainable AI (XAI) Solutions For Data Engineers. NVEO - Natural Volatiles & Essential Oils, 8(3), 425–432.

https://doi.org/https://doi.org/10.53555/nveo.v8i3.5769

[36]. Singirikonda, P., Katikireddi, P. M., & Jaini, S. (2021). Cybersecurity In Devops: Integrating Data Privacy And Ai-Powered Threat Detection For Continuous Delivery. NVEO - Natural Volatiles & Essential Oils, 8(2), 215–216. https://doi.org/https://doi.org/10.53555/nveo.v8i2.5770

[37]. Kilaru, N. B., & Cheemakurthi, S. K. M. (2021). Techniques For Feature Engineering To Improve Ml Model Accuracy. NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO, 194-200.

[38]. Vasa, Y., Jaini, S., & Singirikonda, P. (2021). Design Scalable Data Pipelines For Ai Applications. NVEO - Natural Volatiles & Essential Oils, 8(1), 215–221. https://doi.org/https://doi.org/10.53555/nveo.v8i1.5772

[39]. Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1).96 -102.