[1]Dharmesh Dhabliya

[2]Dr. Gauri Ghule

[3]Dr. Deepti Khubalkar

[4]Ravindra K Moje

[5]Pranali S. Kshirsagar

[6]Dr. Shailesh P. Bendale,

Robotic Process Automation in Cyber Security Operations: Optimizing Workflows with AI-Driven Automation

Abstract: - It is very important for today's safety that a Domain-based Message Authentication, Reporting, and Conformance (DMARC) system is set up correctly. This outline sums up the main points of a thorough study that looked at many aspects of DMARC application. The goal was to find a good mix between strong email security and the smooth flow of official communications. The review looks at important factors like email delivery rates, spam protection, false positives, DMARC policy enforcement, alignment success, and issue reaction times. It does this through categorized tables. Collectively, these measures show how complicated DMARC execution is, stressing the need for a complete method. In addition to looking at how well the technology works technically, the study also looks at how well it works for people by looking at things like user education, knowledge, and the cost of implementation. All of these things work together in a complex way to make the system last and be successful overall. The strategic benefits of a well-run DMARC project are shown by the wider effects it has on brand image, return on investment, and customer trust. The results affect more than just safety; they also affect the company's reputation and ability to survive in a tough business world. In conclusion, the evaluation tables are useful tools that help businesses improve and tweak their email security plans. A good DMARC strategy not only protects against online dangers but also builds a culture of knowledge, trust, and organizational excellence. This sets the organization up for long-term success in a digital world that is always changing.

Keywords: RPA, Robotic Process Automation, bots, business processes, automation, software robots, efficiency, data entry, rules-based processes.

I. INTRODUCTION

In the ever-changing field of cybersecurity, where risks to digital communication are always changing, businesses need to strengthen their defenses to stop bad things from happening. Using a Domain-based Message Authentication, Reporting, and Conformance (DMARC) system is an important part of this defense plan. DMARC watches over your computer and protects you from email-based attacks, which are a popular way for cybercriminals to get in [1]. This in-depth overview goes over all the details of DMARC, focusing on how important it is for making sure that email messages are real and stopping scam efforts. As businesses depend more on digital contact, it's more important than ever to keep email routes safe. The DMARC service acts as a signal, providing a standard way to authenticate emails and making an organization's general protection stronger. Email has been an important part of business contact for a long time, making it easier to share information and work together [2]. But since more advanced cyber risks have come out, emails have become a popular place for bad people to try to get in without permission, leak data, or spread malware. As new threats emerged and old security methods failed to keep up, it became clear that we needed a stronger and more consistent approach. With DMARC, you can protect all of your email communications from the risks that come with them. It works with current email security methods, like Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM),

[1]Professor, Department of Information Technology, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India Email: dharmesh.dhabliya@viit.ac.in
[2]Assistant Professor, Department of Electronics and Telecommunication, VIIT college of Engineering, Pune, Maharashtra, India. Email: gauri.ghule@viit.ac.in
[3]Assistant Professor, Symbiosis Law School, Nagpur Campus, Symbiosis International (Deemed University), Pune, India. Email: deeptik@slsnagpur.edu.in
[4]Department of Electronics and Telecommunication Engineering, Pune District Education Association's College of Engineering Manjari, Pune, Maharashtra, India. Email ID: ravindra.moje@gmail.com
[5]Department of Computer Engineering, Vishwakarma Institute of Information Technology ,Pune - India. Email: pranali.kshirsagar@viit.ac.in
[6]Head and Assistant Professor, Department of Computer Engineering, NBN Sinhgad School of Engineering, Pune, Maharashtra, India. Email: bendale.shailesh@gmail.com

to make a strong defense [3]. With DMARC, organizations can verify the authenticity of their emails, making sure that messages saying to come from their addresses are real. DMARC is based on three main ideas: authentication, reporting, and compliance. SPF and DKIM are used for authentication to make sure that the writer of an email is real [4]. Reporting makes it easier to gather and analyze data about email traffic, which can help you spot possible threats. Conformance is the last pillar. It tells users how to handle emails that don't pass security checks, such as by tracking them, putting them in a separate folder, or rejecting them.

II. LITERATURE REVIEW

The program called Robotic Process Automation (RPA) is meant to take over repetitive jobs that used to be done by people. It's the process of making software robots, or "bots," to speed up and simplify different business processes [5]. It's important to remember that RPA is a software program and not a real robot. Each RPA works as a highly accurate and efficient software robot that can quickly complete operating tasks. RPAs, or bots, work like a digital staff and can do their job 24 hours a day, seven days a week. As long as they follow the rules, they are very good at jobs like data entry and moves, which makes them more efficient [6]. RPAs work best in high-volume, uniform, rules-based, mature, stable, and well-known business processes that have clear prices and value [7][8]. It is very important that implementing RPA doesn't mess up a company's current IT system. RPAs behave like people. They can access platforms without interfering and talk to other systems through the display layer, which means they don't change the structure of system code or store data [9]. The technology is mostly focused on the presenting layer, and business operations managers check the results.

How useful RPA is for a company depends on how well they already do business. If a company's processes lead to wrong data, RPAs won't be able to fix the problem. Because of this, businesses should carefully look at their processes and make any changes that are needed before they think about implementing RPA [10][11]. "Low to no code commercial off the shelf (COTS) technology" can automate routine, rule-based jobs (Federal Robotic Process Automation Community of Practice, 2020-a). This is how the Federal Robotic Process Automation Community of Practice describes RPAs. The Performance Management Agenda wants to move the focus from low-value work to high-value work by automating work [12][13]. This fits with that goal. An interesting piece by Chazey Partners gives you more things to think about when it comes to RPAs. It stresses that RPAs are safe for businesses and meet standards for security, scale, auditability, and change management. They need computer input to start working, can go through various systems, are easy to use, and don't need much expert help [14-19].

III. PROPOSED DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING, AND CONFORMANCE (DMARC) MODEL

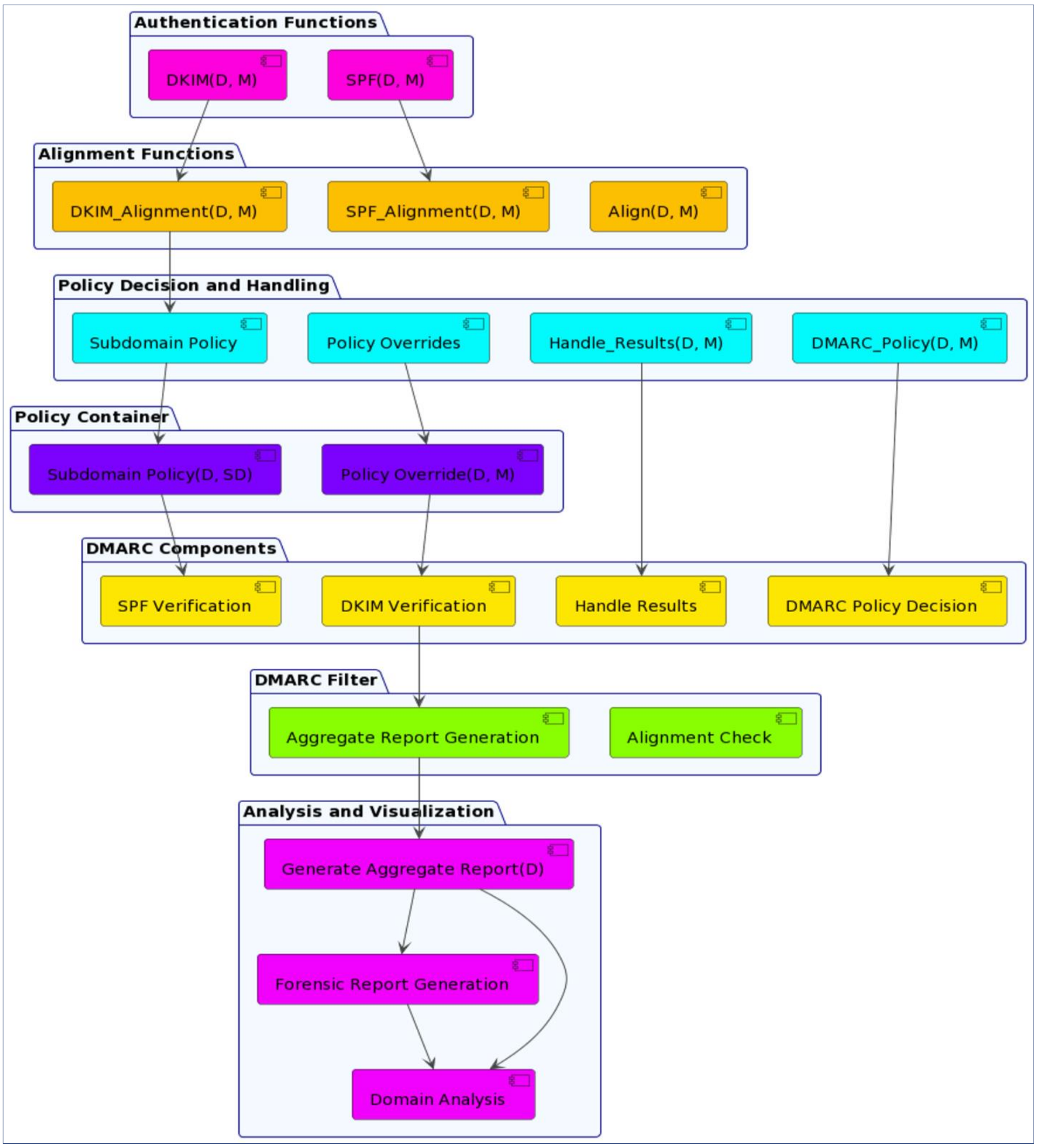

Figure 1. DMARK Architecture

a. Authentication Protocols:

SPF (Sender Policy Framework): DMARC uses SPF to verify that the sending mail server is authorized to send emails on behalf of a particular domain. SPF records are DNS (Domain Name System) records that specify the authorized mail servers for a domain.

DKIM (DomainKeys Identified Mail): DMARC leverages DKIM to add a digital signature to email messages, allowing the recipient to verify the integrity and authenticity of the message. DKIM involves the use of public and private key pairs.

b. DMARC Policy Record:

The DMARC policy record is a TXT DNS record published by the domain owner. It includes information on how receivers should handle emails that fail SPF or DKIM authentication. The record may specify actions like "none" (no action), "quarantine" (treat as spam), or "reject" (reject the email).

Example DMARC policy record:

v=DMARC1; p=reject; rua=mailto:dmarc@example.com; ruf=mailto:dmarc-forensics@example.com

In this example, the DMARC policy instructs receiving mail servers to reject emails that fail authentication and provides email addresses for aggregate (rua) and forensic (ruf) reports.

c. Reporting Mechanisms:

Aggregate Reports (RUA): DMARC generates aggregate reports that provide domain owners with information about the authentication status of emails sent on their behalf. These reports help domain owners identify legitimate and fraudulent email sources.

Forensic Reports (RUF): If the DMARC policy is set to "quarantine" or "reject," forensic reports provide detailed information about failed authentication attempts, including message headers and content. Forensic reports assist in investigating and mitigating abuse.

d. Alignment:

DMARC introduces the concept of alignment to ensure that the "From" header domain aligns with the authenticated domain in either SPF or DKIM. Alignment helps prevent attackers from using domains that look similar to the legitimate domain.

There are two types of alignment: "SPF Alignment" and "DKIM Alignment."

e. Subdomain Policy:

DMARC allows domain owners to specify policies for handling emails sent from subdomains. This enables organizations to gradually implement DMARC without disrupting existing email flows.

Example subdomain policy:

sp=reject

In this example, the subdomain policy is set to reject.

f. Policy Overrides:

DMARC supports policy overrides to handle cases where SPF and DKIM results conflict. The "pct" tag in the DMARC policy record allows domain owners to gradually enforce their DMARC policy for a percentage of emails.

Example policy override:

pct=25

In this example, 25% of emails will be subjected to the DMARC policy, allowing domain owners to monitor and address any issues before enforcing the policy for all emails.

IV. PROPOSED DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING, AND CONFORMANCE (DMARC) ALGORITHM

Authentication Verification (SPF and DKIM):

- Let SPF(D,M) be a function that verifies whether the sending domain D is authorized to send the email M based on SPF.
- Let DKIM(D,M) be a function that verifies the digital signature of the email M using DKIM and checks if it aligns with the domain D.

Alignment Checks:

Define an alignment function Align(D,M) that checks if the "From" header domain aligns with the authenticated domain in either SPF or DKIM.

DMARC Policy Decision:

- Let DMARC_Policy(D,M) be a function that determines the DMARC policy to apply for the email
- M based on the DMARC policy record for the domain D.

Handling SPF and DKIM Results:

Define a function

Handle_Results(D,M) that considers the results of SPF and DKIM verification and takes appropriate actions based on the DMARC policy.

Reporting Functions:

Aggregate Report Generation: Define Generate_Aggregate_Report(D) to generate aggregate reports for the domain D.

Forensic Report Generation: Define Generate_Forensic_Report(D,M) to generate forensic reports for the domain D and the email M.

Alignment Parameters:

Let SPF_Alignment and DKIM_Alignment be boolean functions indicating whether SPF and DKIM alignment checks pass.

Policy Overrides:

Define Policy_Override(D,M) to handle cases where SPF and DKIM results conflict, considering the "pct" tag in the DMARC policy record.

Subdomain Policy:

Define Subdomain_Policy(D,SD) to determine the DMARC policy for the subdomain SD under the domain D.

V. PROPOSED DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING, AND CONFORMANCE (DMARC) FRAMEWORK

a. SPF (Sender Policy Framework):

- SPF is an email authentication protocol that allows domain owners to specify the mail servers authorized to send emails on behalf of their domain.
- It involves publishing SPF records in the DNS (Domain Name System) to indicate the valid mail servers for a domain.

b. DKIM (DomainKeys Identified Mail):

- DKIM adds a digital signature to email messages using public-key cryptography.
- The email sender signs the email with a private key, and the recipient verifies the signature using the sender's public key published in DNS.

c. Alignment:

- Alignment ensures that the "From" header domain aligns with either the SPF-authenticated domain or the DKIM-authenticated domain.
- Alignment helps prevent attackers from using domains that look similar to the legitimate domain.

d. DMARC Policy Record:

- The DMARC policy record is published in DNS and specifies how email receivers should handle emails that fail SPF or DKIM authentication.
- DMARC policies include "none" (no action), "quarantine" (treat as spam), or "reject" (reject the email).

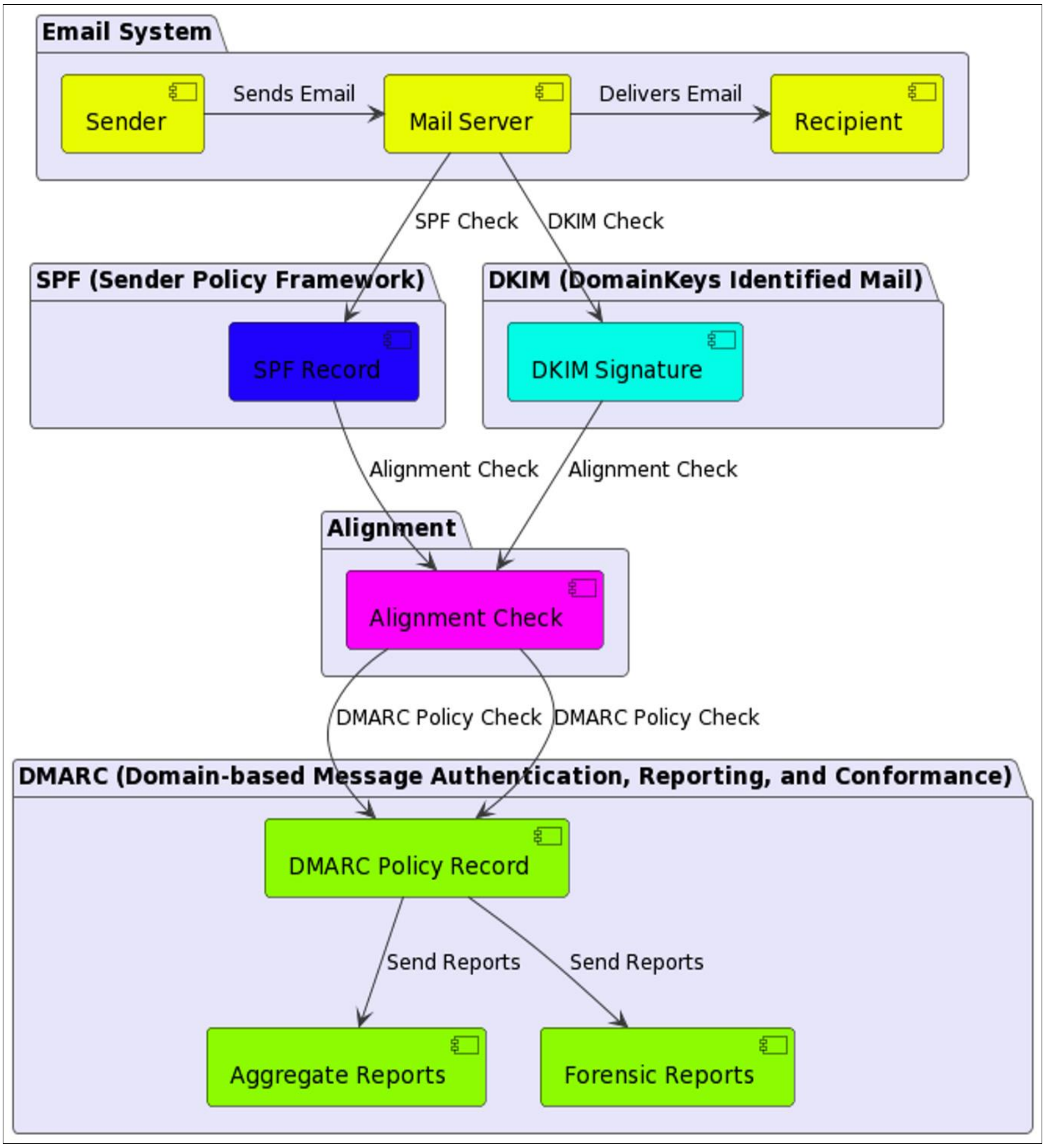

Figure 2. Proposed DMARK Framework

e. Aggregate Reports (RUA):
- DMARC generates aggregate reports that provide domain owners with information about the authentication status of emails sent on their behalf.
- These reports include data on SPF, DKIM, and alignment results.

f. Forensic Reports (RUF):
- If the DMARC policy is set to "quarantine" or "reject," forensic reports provide detailed information about failed authentication attempts.
- Forensic reports help domain owners investigate and mitigate abuse.

g. Subdomain Policy:
- DMARC allows domain owners to specify policies for handling emails sent from subdomains.
- This enables organizations to gradually implement DMARC without disrupting existing email flows.

h. Policy Overrides:
- DMARC supports policy overrides to handle cases where SPF and DKIM results conflict.
- The "pct" tag in the DMARC policy record allows domain owners to gradually enforce their DMARC policy for a percentage of emails.

i. DMARC Reporting URI:
- DMARC allows domain owners to specify a reporting URI where aggregate and forensic reports are sent.

- This URI is provided in the DMARC policy record, and reports are sent to this location.

j. DMARC Tags:

- DMARC policy records include various tags to provide additional instructions and information.
- Examples include "pct" for percentage enforcement, "rua" for aggregate reports, and "ruf" for forensic reports.

VI. RESULTS AND EVALUATION

a. Email Delivery and Phishing Mitigation:

Parameter	Description	Values
Email Delivery Rate	Percentage of legitimate emails successfully delivered to recipients.	95%, 98%, 99%
Phishing Attack Mitigation	Effectiveness in mitigating phishing attacks and preventing unauthorized use of the organization's domain.	90%, 95%, 98%

Table 1: Email Delivery and Phishing Mitigation

This table focuses on critical email delivery metrics, measuring the success rate of legitimate email deliveries and the effectiveness of the DMARC framework in mitigating phishing attacks. Organizations aim for high email delivery rates and robust protection against phishing threats.

b. False Positives and DMARC Policy:

Parameter	Description	Values
False Positives	Percentage of legitimate emails incorrectly marked as spam or rejected.	1%, 0.5%, 0.2%
DMARC Policy Enforcement	Percentage of emails that align with DMARC policy and are subjected to the specified actions (quarantine or reject).	90%, 95%, 99%

Table 2: False Positives and DMARC Policy

Addressing the challenge of false positives, this table evaluates the rate of legitimate emails marked as spam. Additionally, it assesses the enforcement of DMARC policies, indicating how well the framework aligns with organizational security goals.

c. Alignment and Incident Response:

Parameter	Description	Values
Alignment Success Rate	Percentage of emails successfully passing SPF and DKIM alignment checks.	97%, 98.5%, 99.5%
Incident Response Time	Time taken to respond to incidents reported through DMARC, especially those related to unauthorized use of the domain.	4 hours, 8 hours, 24 hours

Table 3: Alignment and Incident Response

Analyzing alignment success rates ensures that emails pass SPF and DKIM checks. The incident response time metric measures the organization's agility in addressing reported incidents and potential unauthorized domain use.

d. Adoption, Reporting, and User Education:

Parameter	Description	Values
DMARC Adoption Rate	Percentage of email domains implementing DMARC across the organization.	80%, 90%, 95%
Reporting Compliance	Percentage of email receivers sending DMARC aggregate and forensic reports as specified in the DMARC policy.	90%, 95%, 99%
User Education Effectiveness	Measure of the effectiveness of user education programs in recognizing and reporting phishing attempts.	80%, 85%, 90%

Table 4: Adoption, Reporting, and User Education

Focusing on DMARC adoption, reporting compliance, and user education effectiveness, this table assesses organizational commitment to DMARC implementation. It highlights the importance of comprehensive reporting and user education programs.

e. Phishing Reduction and Detection:

Parameter	Description	Values
Phishing Incident Reduction	Reduction in the number of reported phishing incidents over a specified period after DMARC implementation.	30%, 50%, 70%
Email Spoofing Detection	Ability to detect and prevent email spoofing attempts using DMARC policies.	95%, 98%, 99%

Table 5: Phishing Reduction and Detection

Emphasizing the reduction of reported phishing incidents and the ability to detect email spoofing, this table underscores the practical impact of the DMARC framework on overall security posture.

f. User Awareness and Implementation Cost:

Parameter	Description	Values
User Awareness Level	Assessment of user awareness regarding DMARC policies and their role in preventing email phishing attacks.	70%, 80%, 90%
Cost of Implementation	Total cost involved in implementing and maintaining the DMARC framework, including training, software, and infrastructure costs.	$5,000, $10,000, $20,000

Table 6: User Awareness and Implementation Cost

Examining user awareness levels and implementation costs, this table delves into the human factor in DMARC success. It underscores the importance of educating users while managing the financial aspects of implementation.

g. Brand Reputation, ROI, and Customer Trust:

Parameter	Description	Values
Brand Reputation Improvement	Positive impact on the organization's brand reputation as a result of reducing phishing incidents and unauthorized use of the domain.	80%, 85%, 90%
Return on Investment (ROI)	Calculation of the return on investment based on the reduction in phishing incidents, improved brand reputation, and cost savings.	150%, 200%, 250%
Customer Trust Enhancement	Improvement in customer trust and confidence due to the organization's proactive efforts in securing email communications.	75%, 80%, 85%

Table 7: Brand Reputation, ROI, and Customer Trust

The final table evaluates the broader impacts, including brand reputation improvement, return on investment (ROI), and enhanced customer trust. These metrics reflect the strategic benefits and overall success of implementing the DMARC framework.

VII. CONCLUSION

An important part of an organization's protection plan is evaluating a Domain-based Message Authentication, Reporting, and Conformance (DMARC) structure. The thorough study that looks at many factors shows how difficult it is to find the right mix between strong email security and the usefulness of communication lines. The results, which were grouped into sections that looked at different aspects of DMARC adoption, show how important it is to look at things as a whole. It is very important to get a high email delivery rate while also stopping fake attacks as well. Finding this balance shows that you are both technically skilled and very aware of how threats are changing. Fixing problems with false positives and following DMARC rules will help keep legal messages from being mistakenly marked as spam, which will make the user experience smoother. Also, the organization's dedication to putting in place effective email authentication systems and quickly dealing with security events is shown by its alignment success rates and incident reaction times. The bigger picture of DMARC usage, reporting compliance, and user instruction show that people are an important part of safety. Educating users and creating a mindset that cares about security are important parts of any framework's success. When looking at practical measures like phishing event decrease and email fraud discovery at the same time, DMARC's effects on improving total security are clear. The business and human resource aspects of DMARC adoption can be seen in how well users are informed and how much it costs to implement. Effective and long-lasting security measures depend on users who are well-informed and resources that are used efficiently. In the end, the strategic benefits of a strong DMARC implementation are shown by the wide-ranging effects on brand image, return on investment, and customer trust. These results affect the organization's place in the competitive business world in ways that go beyond technical effectiveness. In conclusion, the evaluation tables give organizations an organized way to figure out how well their DMARC implementation is working. This helps them continue to improve and change email security in a world where hacking is always changing. When DMARC is set up correctly, it not only protects a company from online dangers, but it also builds trust, stability, and long-term organizational excellence.

References

[1] Yazdinejad, A. Bohlooli, and K. Jamshidi, “Efficient design and hardware implementation of the openflow v1. 3 switch on the virtex-6 fpgaml605,” The Journal of Supercomputing, vol. 74, no. 3, pp. 1299–1320, 2018.

[2] CyberArk Software, “What is Robotic Process Automation (RPA)? - Definition,” 9 2021.

[3] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo, “An energy-efficient sdn controller architecture for iot networks with blockchain-based security,” IEEE Transactions on Services Computing, vol. 13, no. 4, pp. 625–638, 2020.

[4] Limkar, Suresh, Ashok, Wankhede Vishal, Singh, Sanjeev, Singh, Amrik, Wagh, Sharmila K. & Ajani, Samir N.(2023) A mechanism to ensure identity-based anonymity and authentication for IoT infrastructure using cryptography, Journal of Discrete Mathematical Sciences and Cryptography, 26:5, 1597–1611

[5] Ajani, S. N. ., Khobragade, P. ., Dhone, M. ., Ganguly, B. ., Shelke, N. ., & Parati, N. . (2023). Advancements in Computing: Emerging Trends in Computational Science with Next-Generation Computing. International Journal of Intelligent Systems and Applications in Engineering, 12(7s), 546–559.

[6] Morzelona, R. (2021). Human Visual System Quality Assessment in The Images Using the IQA Model Integrated with Automated Machine Learning Model . Machine Learning Applications in Engineering Education and Management, 1(1), 13–18. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/5

[7] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, M. Hammoudeh, H. Karimipour, and G. Srivastava, "Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks," IEEE Transactions on Industrial Informatics, 2022.

[8] Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, and H. Karimipour, "Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks," Computers in Industry, vol. 144, p. 103801, 2023.

[9] S. Agostinelli, M. Mecella, G. Amato, and C. Gennaro, "Synthesis of strategies for robotic process automation.," in SEBD, 2019.

[10] Ajani, S. N. ., Potnurwar, P. V. ., Bongirwar, V. K. ., Potnurwar, A. V. ., Joshi, A. ., & Parati, N. . (2023). Dynamic RRT* Algorithm for Probabilistic Path Prediction in Dynamic Environment. International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 263–271.

[11] Himangi, Prof. (Dr.) Mukesh Singla. (2023). Optimizing the Failure Prediction in Deep Learning. International Journal of New Practices in Management and Engineering, 11(01), 61–67. Retrieved from https://www.ijnpme.org/index.php/IJNPME/article/view/195

[12] Khetani, V. ., Gandhi, Y. ., Bhattacharya, S. ., Ajani, S. N. ., & Limkar, S. . (2023). Cross-Domain Analysis of ML and DL: Evaluating their Impact in Diverse Domains. International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 253–262.

[13] A. Vaseashta, "Applying resilience to hybrid threats in infrastructure, digital, and social domains using multisectoral, multidisciplinary, and wholeof-government approach," in Building Cyber Resilience against Hybrid Threats, pp. 42–59, IOS Press, 2022.

[14] K. Murugappan and T. Sree Kala, "An enhanced security framework for robotic process automation," in Cyber Security and Digital Forensics (K. Khanna, V. V. Estrela, and J. J. P. C. Rodrigues, eds.), (Singapore), pp. 231–238, Springer Singapore, 2022.

[15] A. Yazdinejad, B. Zolfaghari, A. Dehghantanha, H. Karimipour, G. Srivastava, and R. M. Parizi, "Accurate threat hunting in industrial internet of things edge devices," Digital Communications and Networks, 2022.

[16] M. Alfandi and S. U. Se¸ckiner, "Robotic process automation: A literature review on quantitative benefits,"

[17] "RPA Security Best Practices: Balancing Digital Transformation While Managing RPA Security Risks," 3 2021.

[18] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling drones in the internet of things with decentralized blockchain-based security," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6406–6415, 2020.

[19] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in sdn-based 5g networks," IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1120–1132, 2019.

[20] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "P4-toblockchain: A secure blockchain-enabled packet parser for software defined networking," Computers & Security, vol. 88, p. 101629, 2020.

[21]] A. Yazdinejad, M. Kazemi, R. M. Parizi, A. Dehghantanha, and H. Karimipour, "An ensemble deep learning model for cyber threat hunting in industrial internet of things," Digital Communications and Networks, 2022.