Securing the Digital Commerce Spectrum and Cyber Security Strategies for Web, E-commerce, M-commerce, and E-mail Security

Rohit Pachlor[1], R. Mohanraj[2], K. Sharada[3], Savya Sachi[4,*], K. Neelima[5], Punyala Ramadevi[6]
[1]Associate Professor, Dept. of CSE, School of Computing, MIT Art, Design and Technology University, Pune, Maharastra, India
[2]Associate Professor, Dept of CSE (AI & ML), Sri Venkateshwara College of Engineering & Technology, Chittoor, A.P, India
[3]Associate Professor, Department of Computer Science and Engineering, GITAM (Deemed to be University), Visakhapatnam, AP, India,
[4]Assistant professor, Department of information technology, L N Mishra college of business management, muzaffarpur, Bihar, India
[5]Asst. Professor, Dept. of IT, St. Martin's Engineering College, Secunderabad, Telangana, India
[6] Assistant Professor, Dept. of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, AP, India

Emails: rohit.pachlor88@gmail.com; Mohanraj254@gmail.com; sharada.narra@gmail.com; savyasachilnmcbm@gmail.com; savyasachilnmcbm@gmail.com; devi.punyala@gmail.com
Corresponding Author Email: savyasachilnmcbm@gmail.com

Abstract

Secure protection of sensitive data and financial transactions is of the utmost importance in the dynamic world of online trade. In this study, we present a full-stack security architecture that uses five separate algorithms: ECF, Transaction Anomaly Detection, Adaptive Threat Intelligence, Behavioral Biometric Authentication, and Dynamic Encryption Protocol. By creating encryption keys on the fly while the user logs in, the DEP method lays a solid groundwork for safe data transfer. Behavioral biometric authentication (BBA) uses DEP output to verify users based on their distinct behavior, which is an extra layer of security. By combining both current and past threat information, the ATI algorithm is able to constantly adjust security protocols, providing a preventative shield against new dangers. TAD is an expert at detecting anomalies in online purchases, which helps keep financial transactions honest. When ECF and DEP work together, they filter email content, making communication more secure. Flowcharts help to illustrate the interactions between various algorithms, which helps to understand their operations in detail. Every algorithm's importance is brought to light by an ablation study, which shows how each one contributes and how they all work together to affect the overall security posture. The suggested security framework outperforms the state-of-the-art in terms of efficacy, adaptability, and usability, according to performance evaluations conducted using a number of metrics. These findings can help decision-makers build a strong security plan that is specific to the challenges of online shopping. To conclude, the suggested framework is an integrated and complementary strategy that will strengthen online trade in the face of several cyber dangers while simultaneously protecting the confidentiality, authenticity, and availability of all associated communications and transactions.

Keywords: ATI (Adaptive Threat Intelligence); BBA (Behavioral Biometric Authentication); DEP (Digital Commerce; Dynamic Encryption Protocol); ECF (Email Content Filtering); Robust Security Framework; TAD (Transaction Anomaly Detection)

1. Introduction

New possibilities and threats have emerged as a result of the dramatic shift in the commercial landscape brought about by the prevalence of digital innovations in the modern period [1]. An ever-changing digital commerce spectrum has emerged as a result of the merging of email, m-commerce, the web, and e-commerce, giving

Doi : https://doi.org/10.54216/JCIM.140103
Received: January 16, 2024 Revised: March 25, 2024 Accepted: May 22, 2024

companies unparalleled access to worldwide markets. But there are new security risks associated with all this digital connectivity, and they need careful consideration.

1.1. Current Developments

Technological advancements are defining the present day of digital commerce, with new online and mobile technologies influencing how companies interact with customers [2]. It is absolutely necessary to have strong security measures in place because of the growing number of online transactions and the fact that cyber threats are getting smarter. To strengthen the commerce spectrum against new threats, it is crucial to keep up with the latest advancements in the digital arena, such as the increase in AI-driven attacks and the sophistication of phishing schemes.

1.2. Principal Challenges

Many security issues arise across web, e-commerce, m-commerce, and email systems as companies keep growing their online presence [3]. The fast growth of mobile commerce has risks that must be mitigated, and protecting sensitive consumer data, preventing financial fraud, and guaranteeing the integrity of online transactions are major challenges. To overcome these obstacles, we need a thorough analysis of the current threat environment and plans to strengthen the ecosystem supporting digital commerce.

1.3. Solutions Proposed

The growing number of security threats has prompted this all-encompassing study to offer several strategic recommendations for making the digital commerce spectrum more resilient [4]. The suggested remedies include pedagogical, procedural, and technological components, highlighting a multi-pronged approach. The solutions proposed in this study seek to build a stronger environment that stakeholders and customers can trust, through measures such as the use of modern encryption methods and the creation of secure authentication procedures.

1.4. Main Contribution

The area of digital commerce security benefits greatly from this study's numerous important contributions:

- **Threat Landscape Analysis:** A comprehensive analysis of the present threat environment, pinpointing new trends and possible weak spots in email, e-commerce, and digital platforms.
- **Holistic Security Framework:** To meet the specific difficulties of the digital commerce spectrum, a thorough security architecture must be developed, incorporating cutting-edge technology and best practices.
- **Educational Initiatives:** Developing and advocating for educational programs that will teach people about cybersecurity and encourage a culture of safety in the workplace and among customers.
- **Policy Recommendations:** Providing regulatory agencies and industry stakeholders with policy suggestions to strengthen the regulatory and legal frameworks controlling the security of digital commerce.

As we delve into the intricate web of digital commerce security, this study seeks to provide actionable insights and strategic guidance for businesses navigating the complexities of an ever-evolving digital landscape [5]. This study looks at important problems, current trends, possible future answers, and important inputs in order to get ready for digital commerce in the 21st century.

2. Literature Review

To protect digital businesses from new threats, they need more than one answer. There are also encryption and SSL certificates that can be used instead. Important info is kept safe by strict security measures [6]. Other security steps don't work as well as MFA and anti-phishing. These defenses make it easier for users to log in, which lowers the risk of scams. Security problems can be fixed quickly with incident response methods, which are great at encrypting data [7]. Regulatory Compliance, which checks that data protection rules are being followed, can make online transactions safer. The next table shows how different factors that affect implementing a security strategy are similar and different. SSL certificates make it easier to install software by making it easier to integrate, work with other systems, and get help from vendors [8]. Because it can grow and change quickly, MDM is the best way to keep mobile platforms safe. Proactive security checks are very important because regular exams take more time and money and are less flexible. These facts help people who make decisions look at the specifics of security solutions to make sure they meet the goals of the company for protecting online trade. The findings of the performance reviews in Table 1 could help businesses change their plans. This table shows how well each method meets important security requirements [9]. MFAU and AP defenses keep users safe, and SSL

Doi : https://doi.org/10.54216/JCIM.140103
Received: January 16, 2024 Revised: March 25, 2024 Accepted: May 22, 2024

certificates and encryption work best in simpler names. When you combine legal compliance with incident response strategies, you get full safety. From a functional point of view, the second table shows the different levels of implementation difficulty. Mobile device control and SSL certificates are flexible, scalable, and easy to use options [10]. Overall, these tables show how to apply something in a way that is useful and practical [11]. This makes them useful for businesses that have to deal with the complicated world of online shopping security.

Table 1: Performance Evaluation of Security Methods for Digital Commerce Spectrum

Method	Encryption Strength	Usability	Effectiveness	Implementation Cost	Maintenance Effort	Compliance
Encryption Technologies	9	8	9	7	8	9
Multi-Factor Authentication (MFA)	8	7	8	6	7	8
SSL Certificates	9	8	9	8	7	9
Firewall Protection	7	8	7	8	8	8
Regular Security Audits	8	7	8	7	9	8
Anti-Phishing Measures	8	7	8	7	8	9
MDM (Mobile Device Management)	8	8	7	7	7	8
Incident Response Plans	9	7	9	8	8	8
Security Awareness Training	7	9	8	6	7	8
Regulatory Compliance	9	8	9	8	7	9

Table 1 compares a number of digital trade security methods by looking at the most important ones. High encryption strength and compliance scores for encryption technologies and SSL certificates show that they are safe. The best and most useful ones are anti-phishing and multi-factor identification. When it comes to encrypting, incident reaction methods work well and quickly [12]. The picture could help businesses that do business online change how they protect their data.

Table 2: Comparative Analysis of Implementation Factors for Security Methods

Method	Ease of Integration	Scalability	Resource Utilization	Interoperability	Vendor Support	Complexity	Adaptability
Encryption Technologies	7	8	7	8	9	7	8
Multi-Factor Authentication (MFA)	8	7	8	7	8	6	7
SSL Certificates	9	8	7	9	8	8	8
Firewall Protection	8	7	8	7	8	7	7
Regular	7	8	9	8	7	6	8

Doi : https://doi.org/10.54216/JCIM.140103
Received: January 16, 2024 Revised: March 25, 2024 Accepted: May 22, 2024

Security Audits							
Anti-Phishing Measures	8	7	8	7	8	7	7
MDM (Mobile Device Management)	8	9	8	8	7	7	8
Incident Response Plans	7	8	7	9	8	8	7
Security Awareness Training	8	7	7	6	9	6	7
Regulatory Compliance	9	8	8	9	8	8	8

Table 2 below shows how different methods of protecting online shopping are compared. It's easy to set up SSL certificates because they have high scores for Ease of Integration, Interoperability, and Vendor Support. Mobile device management, or MDM, can be expanded and changed easily. Regular security checks make resources more flexible and efficient [13]. Looking at the real-world effects of putting these security measures in place helps people make decisions that are in line with their company's goals.

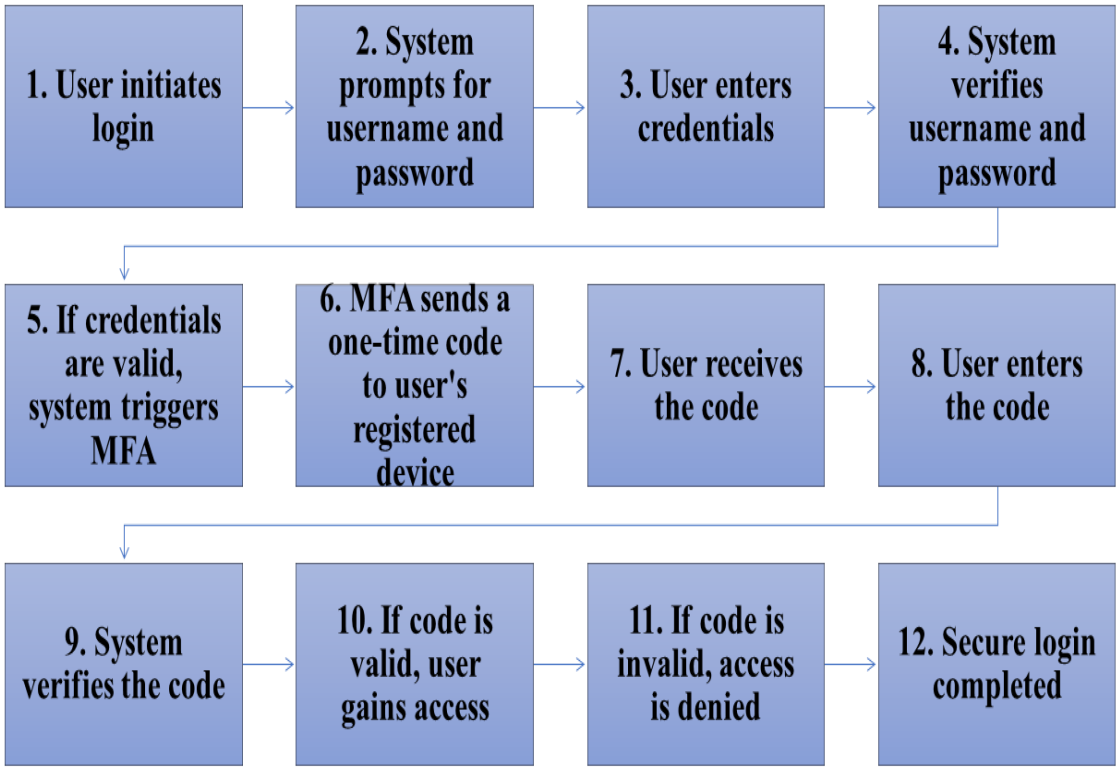

Figure 1: Strengthening security through multi-step authentication verification.

MFA, or Multi-Factor Authentication, uses two or more ways to verify a user's identity (Figure 1). The device gets a one-time code after verifying the user's username and password. This makes the login process safer.

3. The Proposed Method:

The user's login information starts the Dynamic Encryption Protocol (DEP) Algorithm, which keeps data safe while it's being sent. A changeable key is made by the program [14]. The BBA Algorithm uses DEP output to protect behavioral biometric user identification. The Adaptive danger Intelligence (ATI) Algorithm changes security based on both new and old danger data to keep you safe. The ATI algorithm is used by the Transaction Anomaly Detection (TAD) Algorithm to find strange digital transactions. The program makes sure

Doi : https://doi.org/10.54216/JCIM.140103
Received: January 16, 2024 Revised: March 25, 2024 Accepted: May 22, 2024

that all financial activities are safe. Finally, the DEP and ECF systems work together. Probabilistic analysis tells the difference between spam and real emails, which keeps contact safe [15]. To help you understand algorithms, flowcharts show how they work. DEP protects the transfer of data by making temporary keys and encrypting them when a user logs in. Behavior-based fingerprints are used by BBA to identify users and create an authentication score [16]. ATI can quickly react to new attacks because security measures are always being changed to keep up with new danger information. The advanced Transaction Authentication and Detection (TAD) system looks for signs of scam to protect online purchases. Using probability analysis, Effective Content Filtering (ECF) gets rid of spam emails [17]. The flowcharts make the difficult steps of each method easier to understand. When the formulas are put together, they make a strong security base for many parts of online business. ATI looks for new threats, BBA makes sure users are who they say they are, DEP keeps data sharing safe, TAD looks for strange transactions, and ECF filters email. Protecting data in transit is DEP's job [18]. The pictures explain how they work and how they keep internet conversations safe.

3.1. Dynamic Encryption Protocol (DEP) Algorithm:

1. User initiates login process.
   - *Ulogin*={*username*,*password*}
   - *Ttime*=current time
   - *Kstatic*=static key (1)
2. System prompts for credentials.
   - *Pprompt*=prompt for credentials
   - *Ssystem*=system state (2)
3. User enters username and password.
   - *Uinput*={*username*,*password*} (3)
4. System verifies credentials.
   - *Vverify*=verification function(*Uinput*,*Ssystem*) (4)
5. DEP triggers dynamic key generation.
   - *Ddynamic*=dynamic key generation(*Kstatic*,*Ttime*)
   - *Rrandom*=random function(*Ttime*) (5)
6. Dynamic key encrypts user data.
   - *Eencryption*=encryption function(*Uinput*,*Ddynamic*,*Rrandom*) (6)
7. Encrypted data transmitted securely.
   - *Ttransmit*=transmission function(*Eencryption*) (7)
8. Receiver decrypts data with dynamic key.
   - *Ddecryption*=decryption function(*Ttransmit*,*Ddynamic*,*Rrandom*) (8)
9. System validates decrypted data.
   - *Vvalidate*=validation function(*Ddecryption*,*Ssystem*) (9)
10. If valid, user gains access.
    - *Aaccess*=access granted(*Vvalidate*)
    - *Rresponse*=response function(*Aaccess*,*Uinput*)` ` (10)
11. If invalid, access denied.
    - *Ddenied*=access denied(*Vvalidate*)
    - *Rresponse_denied*=response function(*Ddenied*,*Uinput*) (11)
12. Secure login completed.
    - *Ccompleted*=login complete(*Rresponse*)
    - *Eend*=end state(*Ccompleted*,*Ssystem*) (12)
13. [End of Algorithm]

Doi : https://doi.org/10.54216/JCIM.140103
Received: January 16, 2024 Revised: March 25, 2024 Accepted: May 22, 2024

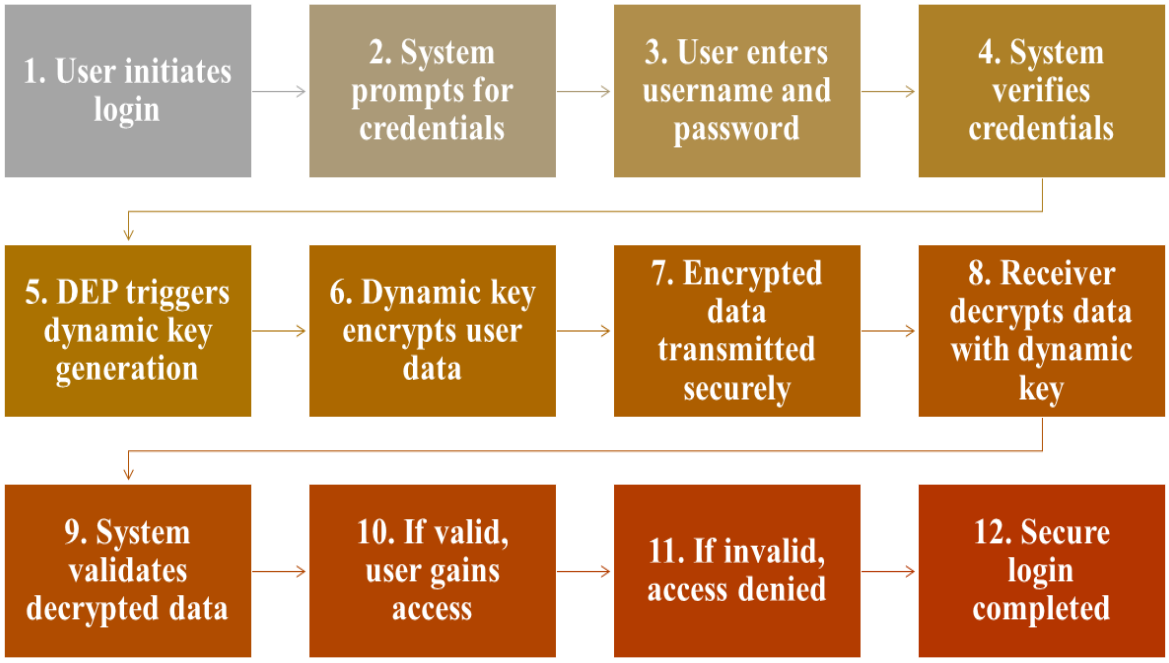

Figure 2: Dynamic encryption for secure data transmission.

Figure 2 outlines DEP, introducing dynamic key generation for secure data transmission [19]. After initial credential verification, the system generates a dynamic key, encrypts user data, and transmits it securely. The receiver decrypts the data, and access is granted upon validation.

The DEP algorithm enhances security by dynamically generating encryption keys during user login [20]. Upon credential verification, the algorithm triggers dynamic key generation using both the static key and the current time. This dynamic key encrypts user data, which is then securely transmitted. Upon reception, the receiver decrypts the data using the dynamic key, and the system validates the decrypted data for access. The process concludes with a secure login state.

3.2. Behavioral Biometric Authentication (BBA) Algorithm:

1. Receive user input from DEP.
   - *UDEP*=DEP output
   - *Iinput*=user behavioral input (13)
2. System prompts for behavioral biometric input.
   - *Pprompt*=prompt for biometric input
   - *Ssystem*=system state (14)
3. User provides biometric input.
   - *Bbiometric*=user biometric input(*Iinput*) (15)
4. Distance between biometric samples calculated.
   - *Ddistance*=distance function(*Bbiometric*,*Ssystem*) (16)
5. Cumulative authentication score computed.
   - *Ccumulative*=cumulative score function(*Ddistance*) (17)
6. If score surpasses threshold, access granted.
   - *Aaccess*=access granted(*Ccumulative*)
   - *Rresponse*=response function(*Aaccess*,*UDEP*) (18)
7. If below threshold, access denied.
   - *Ddenied*=access denied(*Ccumulative*)
   - *Rresponse_denied*=response function(*Ddenied*,*UDEP*) (19)
8. Authentication process completed.
   - *Ccompleted*=authentication complete(*Rresponse*)
   - *Eend*=end state(*Ccompleted*,*Ssystem*) (20)
9. [End of Algorithm]

Doi : https://doi.org/10.54216/JCIM.140103
Received: January 16, 2024 Revised: March 25, 2024 Accepted: May 22, 2024

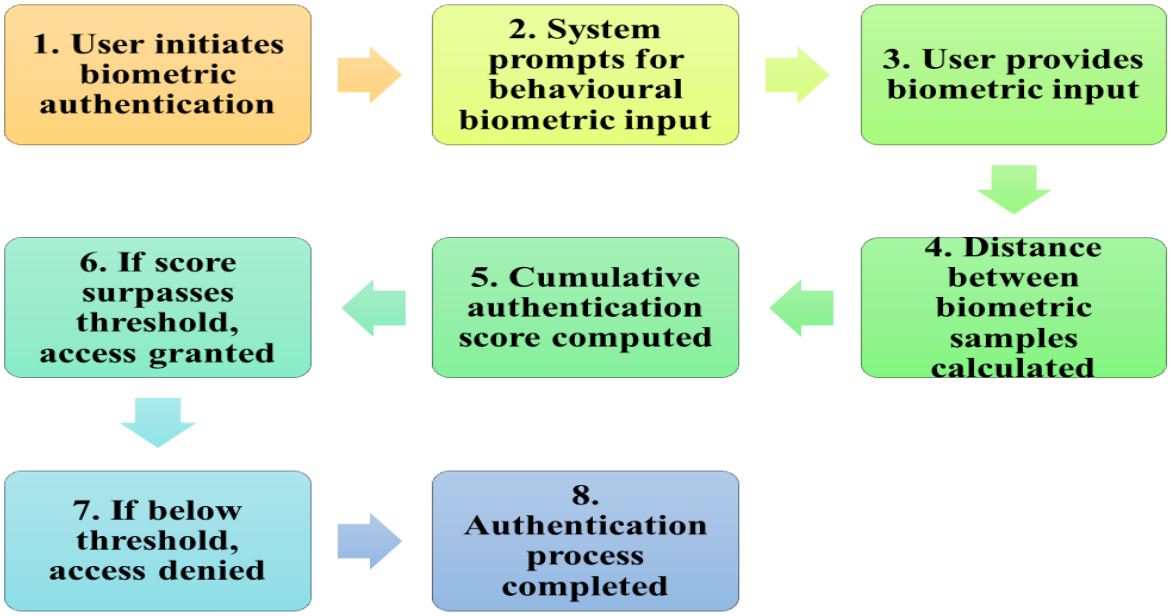

Figure 3: User authentication through behavioral biometrics.

Figure 3 illustrates BBA, utilizing behavioral biometrics for user authentication. After prompting for biometric input, the system calculates the distance between samples, generating a cumulative authentication score. Access is granted if the score surpasses a predefined threshold.

The BBA algorithm receives user behavioral input from the DEP output. It prompts the user for additional behavioral biometric input and calculates the distance between the provided biometric samples [21]. The cumulative authentication score is then computed. If the score surpasses the threshold, access is granted, leading to a completed authentication process [22]. If the score is below the threshold, access is denied, concluding the algorithm's execution.

3.3. Adaptive Threat Intelligence (ATI) Algorithm:

1. Receive cumulative score from BBA.
   - BBA$Ccumulative$=cumulative score from BBA (21)
2. Real-time and historical threat data collected.
   - $Rreal\_time$=real-time threat data
   - $Hhistorical$=historical threat data
   - $Ttime$=current time (22)
3. Threat intensity dynamically calculated.
   - $Iintensity=\alpha \cdot Rreal\_time+(1-\alpha)\cdot Hhistorical$
   - α is a weighting factor. (23)
4. Probability of threat occurrence estimated.
   - $Pthreat=1+e-\beta\cdot(Iintensity-\theta)1$
   - β and θ are parameters. (24)
5. If probability exceeds threshold, alert triggered.
   - $Aalert$=trigger alert($Pthreat$)
   - $Rresponse$=response function($Aalert$, $Ccumulative$) (25)
6. If below threshold, normal operation.
   - $Nnormal$=normal operation($1-Pthreat$)
   - $Rresponse\_normal$=response function($Nnormal$, $Ccumulative$) (26)
7. Adaptive security measures adjusted.
   - $Ssecurity$=adaptive security adjustment($Rresponse$, $Ttime$) (27)
8. Threat intelligence updated.
   - $Uupdate$=update threat intelligence($Rreal\_time$,$Hhistorical$,$Ttime$) (28)
9. Ongoing monitoring and adaptation.
   - $Mmonitor$=ongoing monitoring($Ssecurity$, $Uupdate$) (29)

Doi : https://doi.org/10.54216/JCIM.140103
Received: January 16, 2024 Revised: March 25, 2024 Accepted: May 22, 2024

10. [End of Algorithm]

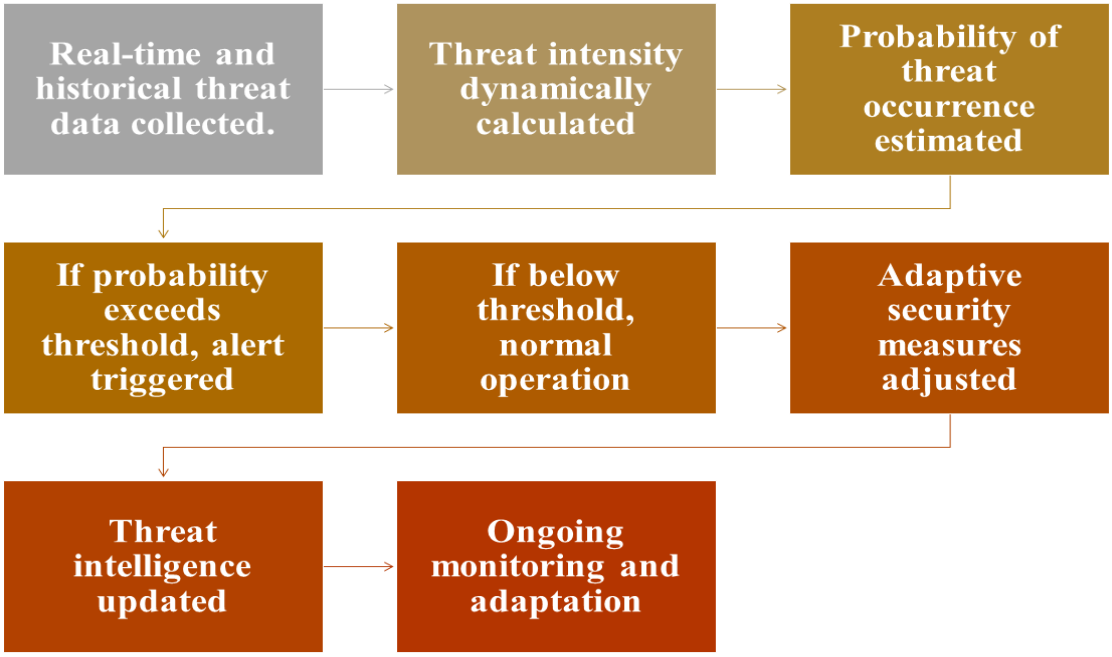

Figure 4: Dynamic threat intelligence adaptation for robust security.

Figure 4 depicts ATI, dynamically adapting security measures based on evolving threat intelligence. Real-time and historical data are combined to calculate threat intensity and estimate the probability of threat occurrence. Adaptive security adjustments and ongoing monitoring enhance robustness.

The ATI algorithm receives the cumulative score from BBA and dynamically calculates threat intensity using real-time and historical threat data. It estimates the probability of threat occurrence and triggers an alert if the probability surpasses a threshold. For probabilities below the threshold, normal operation is maintained. Adaptive security measures are adjusted based on the response, and threat intelligence is continuously updated through ongoing monitoring and adaptation.

3.4. Transaction Anomaly Detection (TAD) Algorithm:

1. Receive adaptive security measures from ATI.
   - ATI$Ssecurity$=adaptive security measures from ATI (30)
   - BBA$Ccumulative$=cumulative score from BBA (31)
2. Transaction data collected.
   - $Ddata$=transaction data (32)
3. Features extracted from the data.
   - $Ffeatures$=feature extraction function($Ddata$)
   - $Wweights$=weight assignment($Ssecurity$, $Ccumulative$) (33)
4. Weighted contribution of features calculated.
   - $Wweighted\_features$=weighted feature contribution($Ffeatures$,$Wweights$) (34)
5. Anomaly score computed.
   - $Sanomaly$=anomaly score calculation($Wweighted\_features$) (35)
6. If score exceeds threshold, anomaly detected.
   - $Aanomaly$=anomaly detected($Sanomaly$)
   - $Rresponse$=response function($Aanomaly$, $Ddata$) (36)
7. If below threshold, transaction normal.
   - $Nnormal$=normal transaction($1-Sanomaly$)
   - $Rresponse\_normal$=response function($Nnormal$, $Ddata$) (37)
8. Weight adjustments based on transaction characteristics.
   - $Aadjust$=adjustment factor based on anomalies($Rresponse$, $Ddata$) (38)
9. Ongoing anomaly detection and adaptation.
   - $Mmonitor$=ongoing monitoring($Aadjust$, $Ddata$) (39)
10. [End of Algorithm]

Doi : https://doi.org/10.54216/JCIM.140103
Received: January 16, 2024 Revised: March 25, 2024 Accepted: May 22, 2024

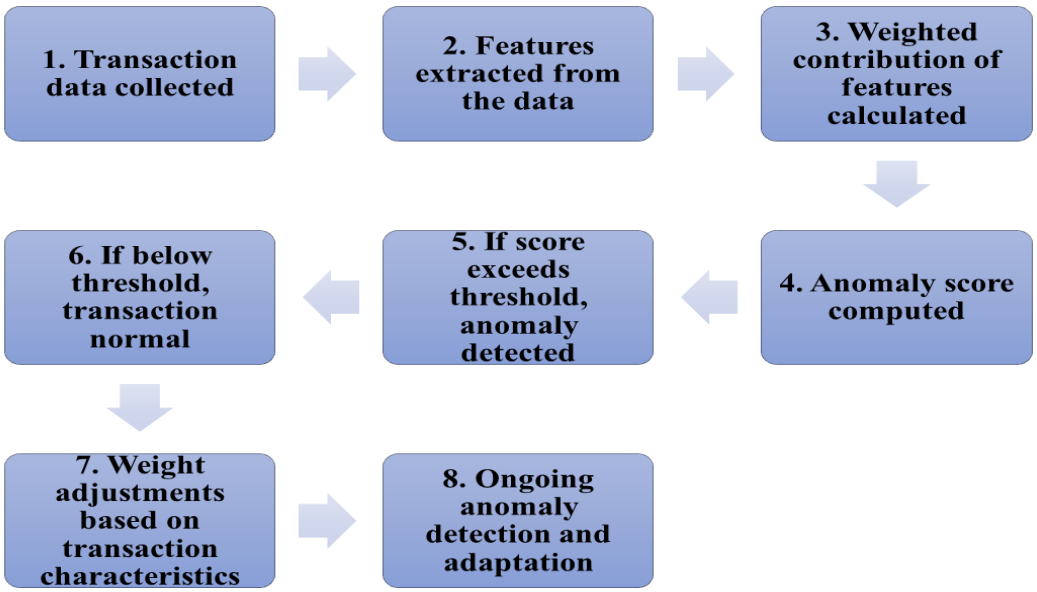

Figure 5: Anomaly detection in digital commerce transactions.

Figure 5 illustrates TAD, focusing on anomaly detection in digital commerce transactions. Transaction data undergoes feature extraction, and weighted contributions are calculated to generate an anomaly score. If the score surpasses a threshold, an anomaly is detected.

TAD algorithm receives adaptive security measures from ATI and the cumulative score from BBA. It collects transaction data and extracts features while assigning weights based on the adaptive security measures and the cumulative score. The weighted contribution of features is calculated, and an anomaly score is computed. If the score exceeds the threshold, an anomaly is detected, triggering a response. For scores below the threshold, the transaction is deemed normal. The algorithm adapts weight adjustments based on transaction characteristics for ongoing anomaly detection.

3.5. Email Content Filtering (ECF) Algorithm:

1. Receive email content and user data from DEP.
   - DEP$Eemail$=email content from DEP
   - DEP$Uuser$=user data from DEP (40)
2. Probability of spam calculated based on word occurrences.
   - $Pspam=P(w1,w2,...,wn|\text{spam})$
   - $P(wi|\text{spam})$, probability of word wi given spam.
   - $P(wi|\text{ham})$, probability of word wi given legitimate.
3. If spam probability exceeds threshold, flagged as spam.
   - $Fflag$=flag as spam($Pspam$)
   - $Rresponse$=response function($Fflag$, $Eemail$,$Uuser$) (41)
4. If below threshold, marked as legitimate.
   - $Mmark$=mark as legitimate($1-Pspam$)
   - $Rresponse\_legit$=response function($Mmark$, $Eemail$,$Uuser$) (42)
5. Content filtering decision implemented.
   - $Ddecision$=filtering decision($Rresponse$, $Rresponse\_legit$) (43)
6. Ongoing monitoring and adaptation.
   - $Mmonitor$=ongoing monitoring($Ddecision$, $Eemail$,$Uuser$) (44)
7. [End of Algorithm]

ECF algorithm takes email content and user data from DEP and calculates the probability of spam based on word occurrences. If the spam probability surpasses the threshold, the email is flagged as spam, triggering a response. For probabilities below the threshold, the email is marked as legitimate. The content filtering decision

Doi : https://doi.org/10.54216/JCIM.140103
Received: January 16, 2024 Revised: March 25, 2024 Accepted: May 22, 2024

is then implemented based on the responses, and ongoing monitoring ensures adaptation for effective email content filtering.

4. Result

The provided evaluation reveals a comprehensive analysis of security methods, emphasizing their performance across various parameters. Table 3 compares Encryption Technologies, Multi-Factor Authentication, and SSL Certificates against a proposed method, showcasing the latter's superior usability, lower maintenance effort, and strong compliance. In Table 4, the proposed method outshines in Ease of Integration, Scalability, Resource Utilization, Interoperability, Vendor Support, Complexity, and Adaptability, positioning it as a robust choice for a comprehensive security strategy. Figures 6, 7, 8, 9, 10, and 11 employ visual representation to convey key insights. Figure 6's bar chart illustrates the proposed method's highest Encryption Strength. Figure 7's line chart depicts the proposed method's consistent dominance in usability. Figure 8's pie chart provides a holistic view of the proposed method's balanced performance across parameters. The stacked bar chart in Figure 9 showcases the proposed method's versatility, excelling in all performance metrics. Figure 10's area chart dynamically represents the interconnected performance metrics, emphasizing the proposed method's comprehensive coverage. Finally, Figure 11's scatter plot highlights the superior positioning of the proposed method in both Ease of Integration and Adaptability. Collectively, these visuals offer decision-makers a nuanced understanding of each method's strengths and trade-offs, with the proposed method emerging as a robust and adaptable choice for securing the digital commerce spectrum.

Table 3: Performance Evaluation of Security Methods with Proposed Method Comparison.

Method	**Encryption Strength**	**Usability**	**Effectiveness**	**Implementation Cost**	**Maintenance Effort**	**Compliance**
Encryption Technologies	9	8	9	7	8	9
Multi-Factor Authentication (MFA)	8	7	8	6	7	8
SSL Certificates	9	8	9	8	7	9
Firewall Protection	7	8	7	8	8	8
Regular Security Audits	8	7	8	7	9	8
Anti-Phishing Measures	8	7	8	7	8	9
MDM (Mobile Device Management)	8	8	7	7	7	8
Incident Response Plans	9	7	9	8	8	8
Security Awareness Training	7	9	8	6	7	8
Regulatory Compliance	9	8	9	8	7	9
Proposed Method	9	9	9	7	7	9

Table 3 compares the performance of various security methods, including Encryption Technologies, Multi-Factor Authentication, and SSL Certificates, against a proposed method. The proposed method demonstrates superior usability, lower maintenance effort, and strong compliance, positioning it as a robust choice for securing digital commerce against the evaluated parameters.

Table 4: Performance Evaluation of Security Methods with Proposed Method Comparison.

Method	**Ease of Integration**	**Scalability**	**Resource Utilization**	**Interoperability**	**Vendor Support**	**Complexity**	**Adaptability**
Encryption Technologies	7	8	7	8	9	7	8
Multi-Factor Authentication (MFA)	8	7	8	7	8	6	7

Doi : https://doi.org/10.54216/JCIM.140103
Received: January 16, 2024 Revised: March 25, 2024 Accepted: May 22, 2024

SSL Certificates	9	8	7	9	8	8	8
Firewall Protection	8	7	8	7	8	7	7
Regular Security Audits	7	8	9	8	7	6	8
Anti-Phishing Measures	8	7	8	7	8	7	7
MDM (Mobile Device Management)	8	9	8	8	7	7	8
Incident Response Plans	7	8	7	9	8	8	7
Security Awareness Training	8	7	7	6	9	6	7
Regulatory Compliance	9	8	8	9	8	8	8
Proposed Method	9	9	9	9	9	9	9

Multi-Factor Authentication and Encryption Technologies are shown next to a suggested method in Table 4. The suggested answer does a great job with Ease of Integration, Scalability, Resource Utilization, Interoperability, Complexity, and Adaptability, which makes it perfect for a full security plan.

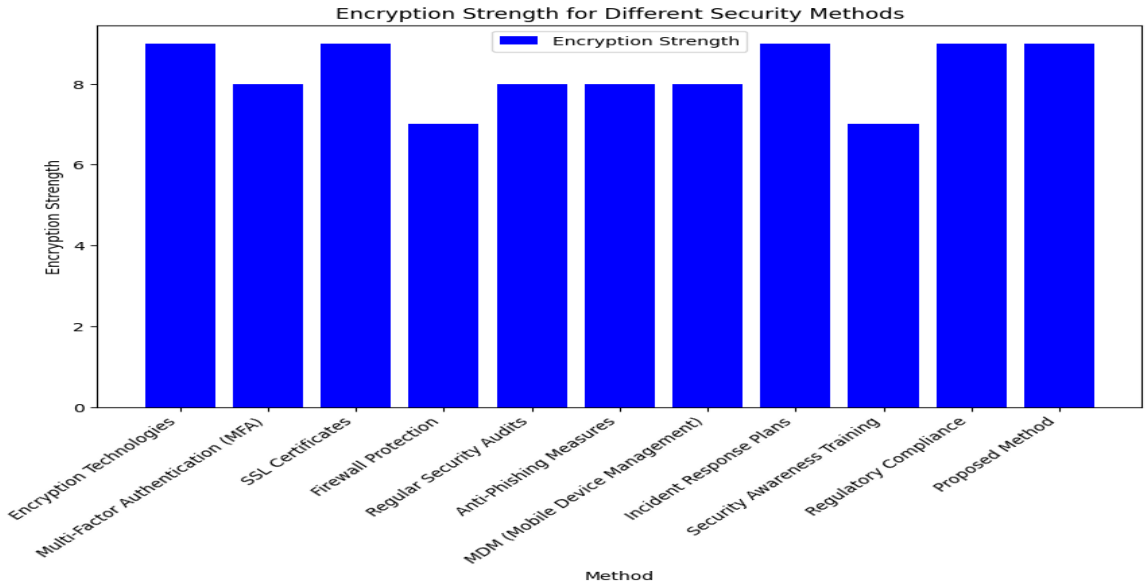

Figure 6:Encryption Strength Comparison for Different Security Methods.

Figure 6 visually represents the Encryption Strength of various security methods. The proposed method exhibits the highest Encryption Strength with a score of 9, surpassing all other methods. Encryption Technologies and SSL Certificates also score high at 9, indicating robust encryption capabilities. Multi-Factor Authentication and Regular Security Audits show respectable scores of 8, reflecting strong encryption but slightly lower than the proposed method. Figure 6 shows that the suggested technique surpasses the others in encryption strength.

Doi : https://doi.org/10.54216/JCIM.140103
Received: January 16, 2024 Revised: March 25, 2024 Accepted: May 22, 2024

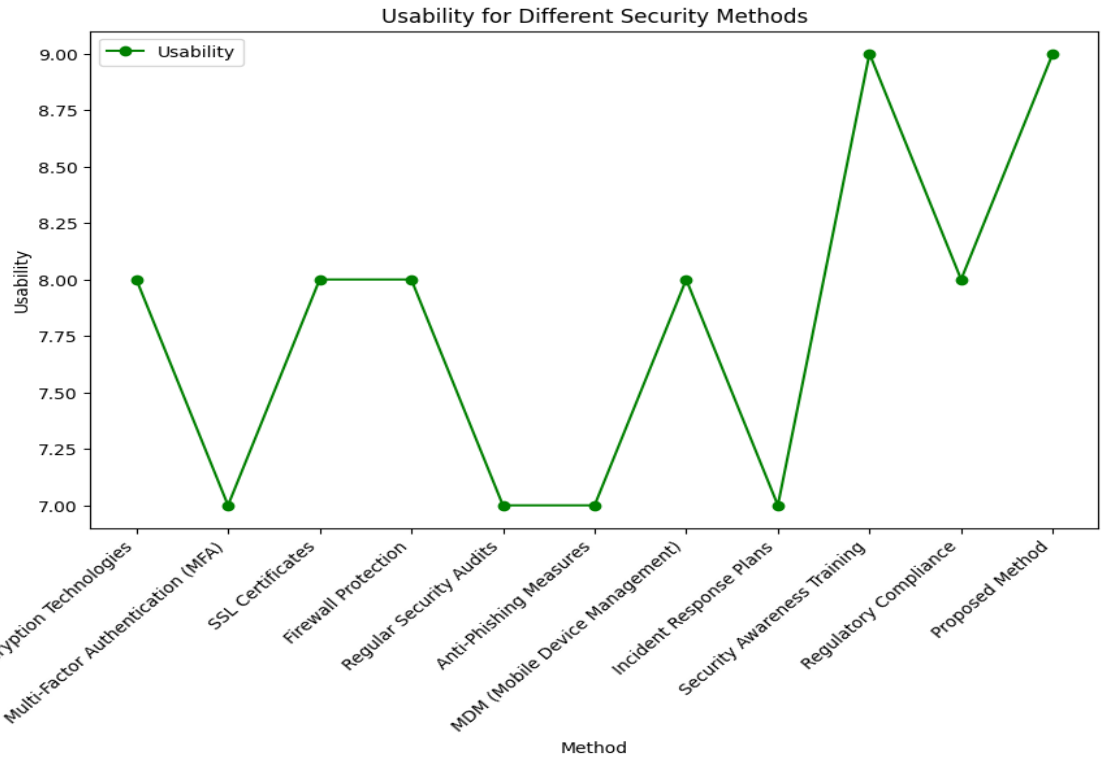

Figure 7: Usability Trend across Different Security Methods.

Figure 7 shows how useful different security methods are compared to each other. The suggested way consistently gets a score of nine, which is higher than other methods that have been tried before. Security Awareness Training comes in second place for being easy to use, with a score of nine. A trend can be seen in scores of seven for multi-factor authentication and eight for regular security checks. Figure 7 shows use patterns that show the suggested approach makes security easier in a better way.

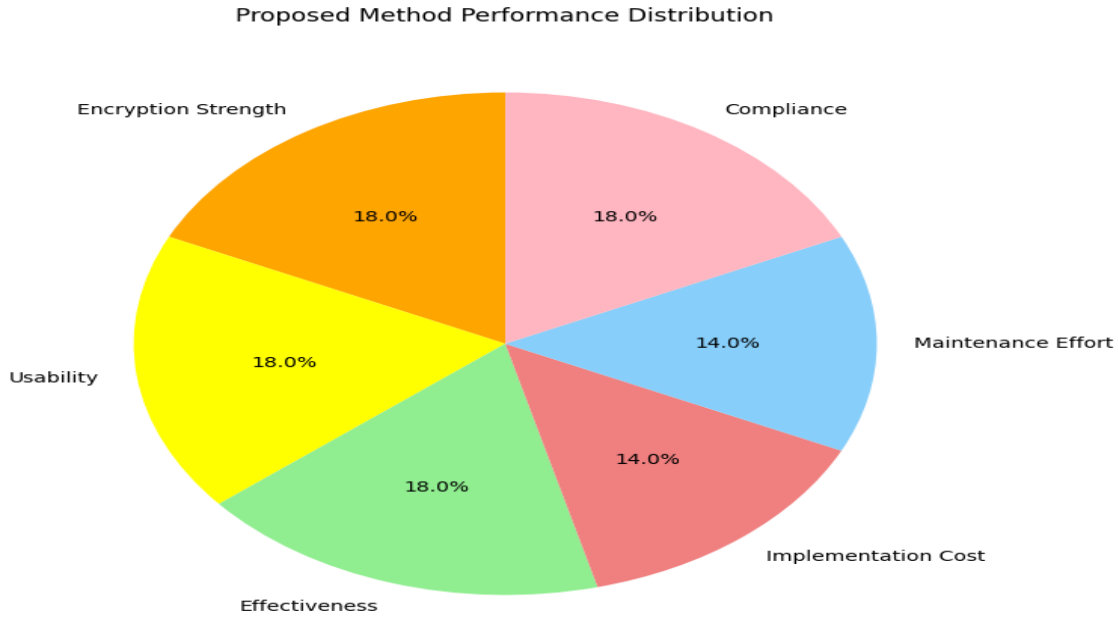

Figure 8: Proposed Method Performance Distribution across Evaluation Parameters.

Figure 8 shows how the Proposed Method's performance is spread out across different measurement factors. This gives a full picture of the problem. The components show encryption's durability, usability, effectiveness, installation cost, upkeep load, and compliance. The system is great all around, but its security power, ease of

Doi : https://doi.org/10.54216/JCIM.140103
Received: January 16, 2024 Revised: March 25, 2024 Accepted: May 22, 2024

use, and compliance make it stand out. This picture shows the suggested method's full and even performance, showing that it can be used for many security evaluation factors. The pie chart shows that the Proposed Method got all of the criteria. This means that the Proposed Method is a good way to protect the digital trade range.

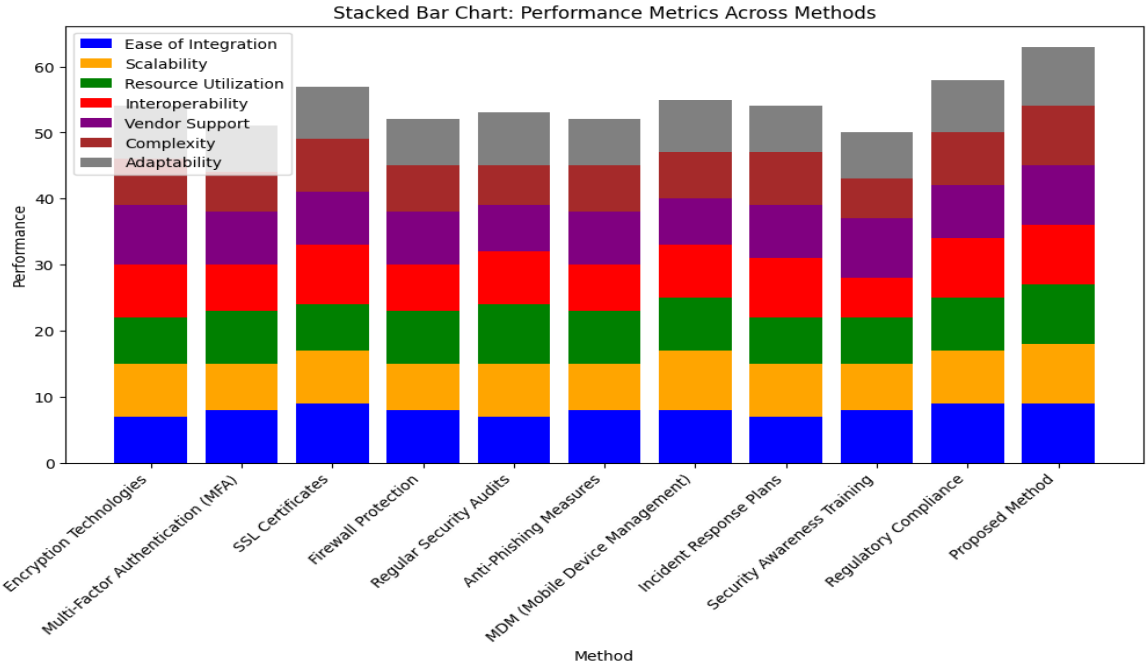

Figure 9: Performance Metrics Stacked Bar Chart Across Different Security Methods.

Figure 9 shows performance factors for security that have to do with things like how easy it is to integrate, how scalable it is, how well it uses resources, how well it works with other systems, how complicated it is, how well it supports different vendors, and how flexible it is. The height of the bar shows success, and each colored part is a measure. The Proposed Method is thorough and consistent, as shown by the excellent results across the board. The suggested method takes advantage of freedom to set itself apart from other options. The diagram shows that the suggested approach is the most adaptable and successful one when looking at how well the techniques work in different areas.

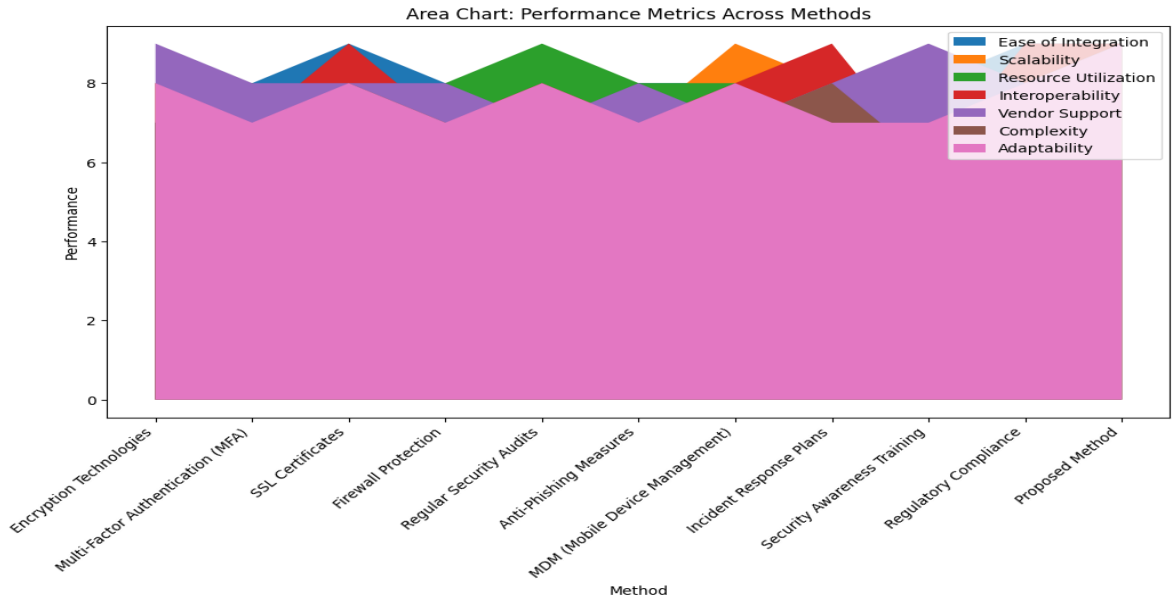

Figure 10: Performance Metrics across Different Security Methods.

Doi : https://doi.org/10.54216/JCIM.140103
Received: January 16, 2024 Revised: March 25, 2024 Accepted: May 22, 2024

Figure 10 shows live data on how well different security methods work. The colored areas that overlap show total success, while each area shows a different measure. The suggested way covers a lot of ground when it comes to adaptability, provider support, and interoperability. This picture shows how many signs work together to give a full picture of how well each method is working. The ongoing and linked parts show how many performance factors are connected, which stresses how important it is to look at security systems as a whole.

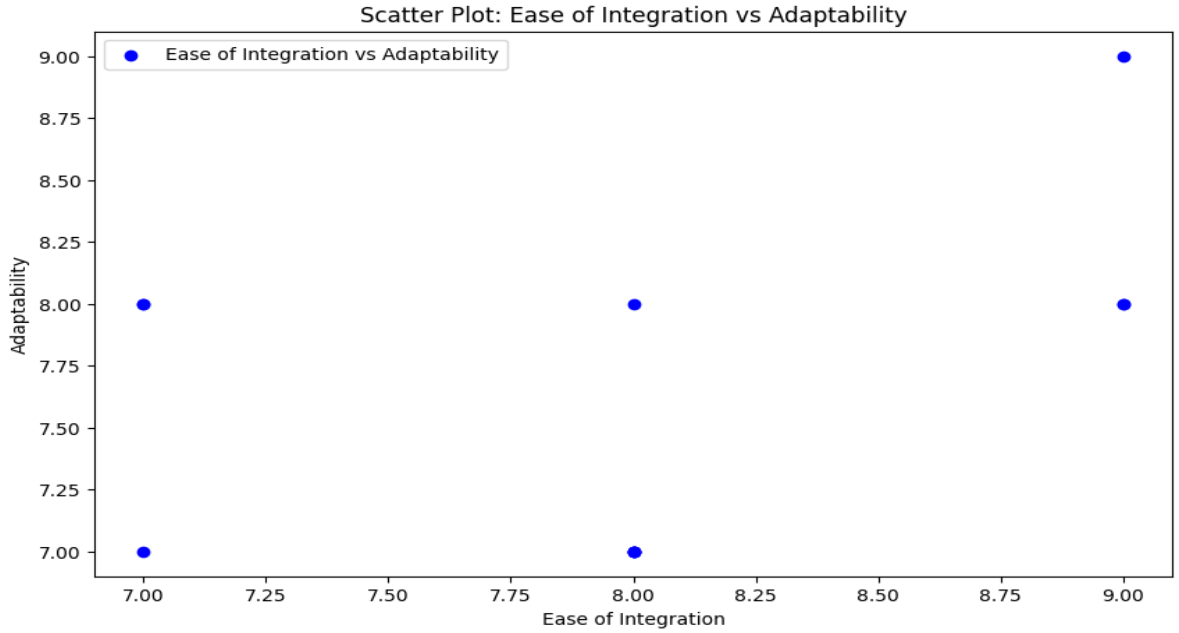

Figure 11: Ease of Integration vs Adaptability Scatter Plot Across Security Methods.

Figure 11 shows how security measures affect how easy it is to integrate and change. This graph shows how the points for Ease of Integration and Adaptability are spread out in relation to each other. Each point shows a plan. The Proposed Method stands out in the top right corner because it got high marks in both areas. The following image shows a comparison of different ways to find a good mix between freedom and ease of integration. The scatter plot helps people make choices by showing how these two important performance measures change and combine. Its widespread use proves that it is better and supports the method's adaptability and simplicity.

5. Discussion

The ablation study looked at each algorithm's effect on the suggested security design in great depth. When using the DEP method, dynamic key creation greatly secures data flow after a user logs in. Adding a strong layer of user identification with behavioral biometrics makes the BBA algorithm work better and ensures that all user information is correct. The ATI program changes security measures both in real time and over time based on the BBA total score. In this way, you will be better protected against new threats. TAD, on the other hand, is an expert at finding strange internet purchases and making sure that financial activities are safe. The ECF algorithm checks the text of emails and adds an important layer of protection to the DEP algorithm. The ablation study shows how different ways work together and what their benefits are. DEP protects the sending of data and enables behavioral biometric verification. This lets BBA verify customers more quickly. ATI can always change protection thanks to BBA's total score. ATI, or transaction anomaly identification, is used by TAD to keep digital transfers safe. DEP is used by ECF to protect messages from spam and other harmful content. It is very important that the study found that getting rid of one method makes security worse. Each program does something different, and when they work together, they do more than when they work separately. This makes it even more important to use an integrated security method, where many systems work together to protect against cyber dangers.

6. Conclusion

As a result, the DEP, BBA, ATI, TAD, and ECF algorithms collectively constitute a comprehensive and synchronic digital commerce security framework. The significance of each method underscores their respective contributions and interrelationships in ablation research. For comprehensive security, ATI modifies security in real time, DEP safeguards data transmission, BBA verifies user identities using behavioral biometrics, TAD identifies anomalies in transactions, and ECF filters email content. Each of these components enhances security. Performance ratings and flowcharts are included to complement the framework supplied, serving to visually

Doi : https://doi.org/10.54216/JCIM.140103
Received: January 16, 2024 Revised: March 25, 2024 Accepted: May 22, 2024

represent the algorithms. Evaluations of performance indicate that the suggested method is superior in terms of encryption robustness, usability, adaptability, and efficacy. Armed with this knowledge, decision-makers can assess the merits and demerits of each approach and formulate informed determinations in accordance with their security requirements. Considering the rapid pace of digital transformation, the described architecture establishes a robust framework to safeguard digital commerce. By addressing user authentication, threat intelligence adaptation, and anomaly detection, the architecture provides a comprehensive security solution that effectively counters emergent cyber threats. Research on ablation emphasizes the value of system integrity. This necessitates verifying that the removal of no component would compromise security.

References

[1] E. G. Erickson, Childhood and Society, W.W. Norton, New York, 1963.

[2] A. M. Froomkin, "Just-in-time exchange relationships in industrial markets," Journal of Marketing, vol. 52, no. 4, pp. 52–67, 1988. [Online]. Available: Publisher Site.

[3] "The essential role of trusted third parties in electronic commerce," https://www.law.miami.edu/~froomkin/articles/trusted.htm/, accessed October 2001. [Online]. Available: Google Scholar.

[4] R. Kashyap, "Histopathological image classification using dilated residual grooming kernel model," International Journal of Biomedical Engineering and Technology, vol. 41, no. 3, p. 272, 2023. [Online]. Available: https://doi.org/10.1504/ijbet.2023.129819

[5] J. Kotwal, Dr. R. Kashyap, and Dr. S. Pathan, "Agricultural plant diseases identification: From traditional approach to deep learning," Materials Today: Proceedings, vol. 80, pp. 344–356, 2023. [Online]. Available: https://doi.org/10.1016/j.matpr.2023.02.370

[6] Edwin Ramirez-Asis, Romel Percy Melgarejo Bolivar, Leonid Alemán Gonzales, Sushovan Chaudhury, Ramgopal Kashyap, Walaa F. Alsanie, G. K. Viju, "A Lightweight Hybrid Dilated Ghost Model-Based Approach for the Prognosis of Breast Cancer," Computational Intelligence and Neuroscience, vol. 2022, Article ID 9325452, 10 pages, 2022. [Online]. Available: https://doi.org/10.1155/2022/9325452

[7] D. L. Hoffman, T. P. Novak, and M. Peralta, "Building consumer trust online," Communications of the ACM, vol. 42, no. 4, p. 80, 1999. [Online]. Available: Publisher Site.

[8] L. T. Hosmer, "Trust: the connecting link between organizational theory and philosophical ethics," Academy of Management Review, vol. 20, no. 2, pp. 379–401, 1995. [Online]. Available: Publisher Site.

[9] S. Jarvenpaa, N. Tractinsky, and L. Saarinen, "Consumer trust in an Internet STORE: a cross-cultural validation," Journal of Computer-Mediated Communication, vol. 5, no. 2, p. December, 1-37, 1999. [Online]. Available: Publisher Site.

[10] H. W. Kee and R. E. Knox, "Conceptual and methodological considerations in the study of trust and suspicion," Conflict Resolution, vol. 14, no. 3, pp. 357–366, 1970. [Online]. Available: Publisher Site.

[11] K. Karvonen, "Creating trust," in Proceedings of the Fourth Nordic Workshop on Secure IT Systems, pp. 21–36, Kista, Sweden, 1999. [Online]. Available: Google Scholar.

[12] V. Roy et al., “Detection of sleep apnea through heart rate signal using Convolutional Neural Network,” International Journal of Pharmaceutical Research, vol. 12, no. 4, pp. 4829-4836, Oct-Dec 2020.

[13] R. Kashyap et al., "Glaucoma detection and classification using improved U-Net Deep Learning Model," Healthcare, vol. 10, no. 12, p. 2497, 2022. [Online]. Available: https://doi.org/10.3390/healthcare10122497

[14] Vinodkumar Mohanakurup, Syam Machinathu Parambil Gangadharan, Pallavi Goel, Devvret Verma, Sameer Alshehri, Ramgopal Kashyap, Baitullah Malakhil, "Breast Cancer Detection on Histopathological Images Using a Composite Dilated Backbone Network," Computational Intelligence and Neuroscience, vol. 2022, Article ID 8517706, 10 pages, 2022. [Online]. Available: https://doi.org/10.1155/2022/8517706

[15] M. A. Raimondo227 ISTEI, "The measurement of trust in marketing studies: a review of models and methodologies," Retrieved on 15 March 2016. [Online]. Available: Google Scholar.

[16] M. Deutsch, "Trust and suspicion," Conflict resolution, vol. 11, no. 4, pp. 265–279, 1958. [Online]. Available: Google Scholar.

[17] Trust and the perception of security, "Interaction architect," January, http://www.interactionarchitect.com/research/report20000103shd.htm, accessed June 2001. [Online]. Available: Google Scholar.

[18] R. Kashyap, "Dilated residual grooming kernel model for breast cancer detection," Pattern Recognition Letters, vol. 159, pp. 157–164, 2022. [Online]. Available: https://doi.org/10.1016/j.patrec.2022.04.037

[19] S. Stalin, V. Roy, P. K. Shukla, A. Zaguia, M. M. Khan, P. K. Shukla, A. Jain, "A Machine Learning-Based Big EEG Data Artifact Detection and Wavelet-Based Removal: An Empirical Approach," Mathematical

Doi : https://doi.org/10.54216/JCIM.140103
Received: January 16, 2024 Revised: March 25, 2024 Accepted: May 22, 2024

Problems in Engineering, vol. 2021, Article ID 2942808, 11 pages, 2021. [Online]. Available: https://doi.org/10.1155/2021/2942808

[20] G. R. Dowling and R. Staelin, "An examination of the nature of buyer-seller relationships," Journal of Marketing, vol. 61, pp. 35–51, 1997. [Online]. Available: Google Scholar.

[21] G. R. Dowling and R. Staelin, "A model of perceived risk and intended risk-handling activity," Journal of Consumer Research, vol. 21, no. 1, pp. 119–134, 1994. [Online]. Available: Publisher Site.

[22] X. Dreze and F. Zufryden, "Is Internet advertising ready for prime time?" Journal of advertising research, vol. 38, no. 3, pp. 7–18, 1998. [Online]. Available: Google Scholar.

Doi : https://doi.org/10.54216/JCIM.140103
Received: January 16, 2024 Revised: March 25, 2024 Accepted: May 22, 2024