Journal of Information Systems Engineering and Management
2025, 10(13s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cybersecurity Threats in Digital Payment Systems (DPS): A Data Science Perspective

Dr. Sheela Hundekari[1], Dr. Jyoti Upadhyay[2], Dr. Anurag Shrivastava[3], Guntaj J[4], Saloni Bansal[5], Alok Jain[6]

[1]*Associate Professor, School of Computer Applications, Pimpri Chinchwad University, Pune. sheela.hundekari@pcu.edu.in*

[2]*Associate Professor, Dept of Computer Science, G.D. Rungta College of Science and Technology, Bhilai, CG*

[3]*Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamilnadu*

[4]*Centre of Research Impact and Outcome, Chitkara University, Rajpura- 140417, Punjab, India*

[5]*Department of Computer Engineering and Applications, GLA University, Mathura*

[6]*Lovely Professional University, Phagwara, India*

ARTICLE INFO

Received: 01 Dec 2024
Revised: 15 Jan 2025
Accepted: 30 Jan 2025

ABSTRACT

The growing dependence on digital payment systems has resulted in a rise in cyber-attacks, therefore endangering user confidence and financial stability. Understanding these threats, evaluating their effect, and investigating data-driven solutions for reducing cybersecurity risks drives this research. The purpose of the study is to explore the cybersecutiy threats in digital payment systems (DPS) and the role of data science techniques in threat detection and prevention. The technique used in the current study is Exploratory Factor Analysis (EFA). It was found that the following are the three key factors reflecting cybersecurity threats i.e., Data Breach & Privacy Threats, Network & System Vulnerabilities, and Fraud & Identity Theft Threats. Data science finds threats, analyzes patterns, and supports proactive defensive mechanisms through Machine learning (ML) algorithms such as anomaly detection, neural networks, and decision trees.

Keywords: Cybersecurity, Digital payment system (DPS), Machine Learning.

INTRODUCTION

Digital payments have generated a lot of buzz around the globe, its importance has grown recently. Both the government and the business sector admit their increasing relevance and are fully using technology. Digital payments have become common as new technology develops and worldwide trade becomes more sought after. Changes in information and communication technology (ICT) have affected behavior and way of life both personally and in businesses. Particularly with relation to organizational performance and operating expenses, ICT has fundamentally impacted economics and finance. The explosive development of ICT in money transactions and settlement is driving a dynamic change in the banking sector. Electronic media is driving a less cash payment scene using transactions, therefore lowering the need of actual money banknotes (Al-Laham et al. 2009).

Various security events including “unauthorized access, malware attack, zeroday attack, data breach, denial of service (DoS), social engineering or phishing, etc.” have expanded at an exponential rate in recent years due to growing reliance on digitalization and Internet-of- Tings (IoT). For example, the security community knew less than 50 million distinct malware executables in 2010. They were double about 100 million by 2012; in 2019, the security community knows of more than 900 million malicious executables; this count is probably going to rise as the technologies progress. (Sarker, I. H., et al. 2020)

1.1 Cybersecurity

Cybersecurity begins with the simple presumption that everyone in cyberspace a broad name for any online or electronic platforms is a desirable target for cybercrime. Our money or data might be the intended objects, but among others spans from usernames, passwords, documents, emails, internet presence. While tailored assaults can exist, most cyberattacks are generic and may happen to anybody. Human mistake is one fundamental and often occurring facilitator of cyberattacks. These enablers may range from the simplistic act of believing electronically transmitted instructions in a phishing email to the more intricate deception of criminals impersonating clients, vendors, or even

workers and professionals seeking access to your assets, both financial and otherwise. Consequently, computer protection against these assaults is rather important. (Sule, et al. 2021).

Cybersecurity is applicable across several domains, including business and mobile computing, and may be categorized into several fundamental types. Information security primarily addresses the protection and confidentiality of relevant data; application security emphasizes safeguarding software and devices from vulnerabilities or cyber threats; network security concentrates on defending computer networks against cyber attackers or intruders; operational security encompasses the protocols for managing and safeguarding data assets. Typical cybersecurity systems generally comprise “network security systems and computer security systems, including a firewall, antivirus software, or an intrusion detection system.” **Sarker, I. H., et al. (2020)**

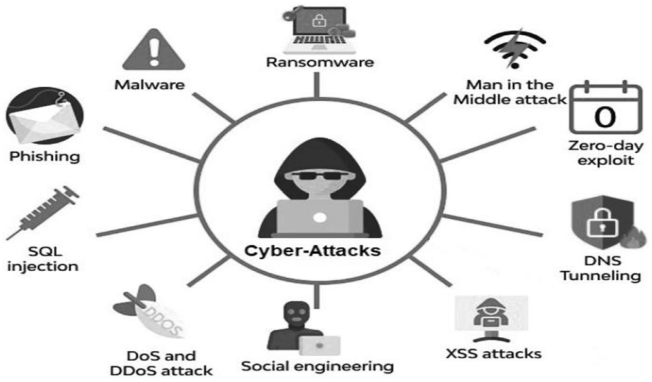


Figure No: 1 Cyber Attacks

Along with affecting companies and people, cybercrime and assaults can result in catastrophic financial losses. Designed to guard computers, networks, programs, and data from assault, damage, or illegal access, cybersecurity is a suite of technologies and procedures (Aftergood, S. 2017). Cybersecurity is experiencing significant technological and operational changes in the framework of computers in recent days; data science (DS) is driving the transition, where machine learning (ML), a fundamental component of "Artifcial Intelligence" (AI) may be rather important to uncover the insights from data. While data science is guiding a new scientifc paradigm and machine learning can significantly alter the cybersecurity scene (Hey, et al. 2009; Cukier, 2010).

1.2 Digital Payment Systems

Digital payments are made using currencies that are comparable to those used in digital media. In addition to making financial investments and a variety of other associated financial products and services, they can be used to buy goods and services. Digital payments are gradually overtaking traditional cash payments because of their traceability, security, convenience, and immediacy (Khando, K.rt al. (2022). Payment methods available to consumers include digital wallets, banks, credit cards, smartphone apps, and cryptocurrency. People are using digital payments more and more, and because they allow consumers to transact globally without being constrained by time or location, they are becoming more and more popular worldwide. The growth of finance also encourages the development of digital payments because it necessitates that investors conduct large-scale transactions involving large sums of money. However, traditional methods of transaction are too tedious and the new digital payment system largely addresses this issue. People will select faster and more convenient payment methods as more people need to pay, hence digital payments will start to gain popularity in response to consumer demand.

There are several types of digital payment systems, each offering different functionalities to suit the needs of consumers and businesses. Some common types include:

Mobile Wallets (E-Wallets): Paytm, PhonePe, Google Pay, and Amazon Pay

Online Banking (Net Banking): Transfer funds, pay bills, and access other banking services online.

UPI (Unified Payments Interface): UPI is a flagship digital payment system in India, introduced by the National Payments Corporation of India (NPCI).

Credit/Debit Cards: Visa, Mastercard, and Rupay

QR Code Payments: PhonePe, Paytm, Google Pay, and BHIM offering QR code-based transactions, especially in small businesses and retail shops.

Digital Bank Transfers: IMPS (Immediate Payment Service), NEFT (National Electronic Funds Transfer), and RTGS (Real-Time Gross Settlement).

Cryptocurrency Payments: Bitcoin, Ethereum, etc. are legally ambiguous in India, some platforms and services do allow users to buy, sell, and use cryptocurrencies. :

Buy Now, Pay Later (BNPL): Simpl, LazyPay, Cashify PayLater, and Amazon Pay Later

Digital Payment Gateways: Razorpay, Paytm Payment Gateway, Instamojo, Citrus Pay, and Stripe

Cybercrime Threats in Digital Payment Systems

Threat Category	Threat Description	Countermeasures
Malware & Phishing Attacks	Malicious software intercepts transactions, steals login credentials; Phishing emails and fake websites trick users.	User education, MFA, security updates, fraud detection, encryption.
Malware Attacks	Mobile Malware: Targets smartphones/tablets to steal transaction data.	Install security software, update OS/apps, avoid unknown downloads.
Phishing Attacks	Fake Apps/Websites: Look-alike platforms steal user credentials. Social Engineering: Impersonation to trick users into revealing data.	Verify app sources, avoid clicking suspicious links, enable 2FA.
Data Breaches & Identity Theft	Attackers exploit system vulnerabilities to steal sensitive user data. Stolen data is used for identity fraud.	Strong encryption, security audits, compliance with data protection laws, user awareness.
Unauthorized Access & Account Takeover	Attackers gain access via brute force, credential stuffing, phishing, SIM swapping.	MFA, constant monitoring, user education, fraud detection, security controls.
NFC & Contactless Payment Risks	Signal Interception: Attackers steal payment data. Relay Attacks & Malicious Tags: Fraudulent transactions via fake NFC devices.	Encryption, tokenization, device authentication, transaction approval, secure elements

Source: Lakshmi, R., & Rani, S. (2024). Securing digital wallets: threats and countermeasures. mLAC Journal for Arts Commerce and Sciences (m-JACS), 2(4), 25–32. https://doi.org/10.59415/mjacs.v2i4.185

1.3 Data Science

Data science is fundamentally concerned with the comprehension of data. Studying, processing, and extracting valuable insights from a collection of information are all components of this process. In addition to data mining, data analytics is also associated with data science. Together with the original data analysis and descriptive analytics from a statistical perspective, the general concept of "data analytics" is formed by the development of data mining, knowledge discovery, and machine learning, which refers to the creation of algorithms and programs that learn on their own. Cao, L. (2017). Many researchers now use the term "data science" to denote the interdisciplinary field of data acquisition, preprocessing, inference, or decision-making through data analysis. The utilization of a variety of

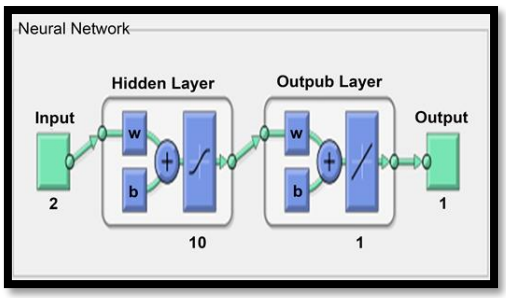
scientific methods, machine learning techniques, processes, and systems is essential for the comprehension and analysis of actual phenomena using data. This field is commonly referred to as data science. "Data science is a novel interdisciplinary field that integrates and expands upon statistics, informatics, computing, communication, management, and sociology to investigate data and its surroundings and to convert data into insights and decisions by adhering to a data-to-knowledge-to-wisdom methodology," as stated by Cao (2017).

1.4 Role of Data Science in Cybersecurity Threat Detection and Prevention

Data science is essential for improving the security of digital payment systems by identifying fraudulent actions, discovering security flaws, and avoiding cyber attacks in real-time. Machine learning (ML) methods, including anomaly detection, neural networks, and decision trees, can detect fraudulent transactions by examining patterns and behavioral irregularities. AI-powered fraud detection helps avert phishing attempts, identity theft, and illegal access. Moreover, blockchain technology guarantees safe and transparent financial transactions, mitigating the dangers of data manipulation and fraud. Utilizing big data analytics, predictive modeling, and automated security frameworks, digital payment systems may improve security, mitigate financial risks, and foster customer confidence in online transactions.

1.4.1 Neural Networks

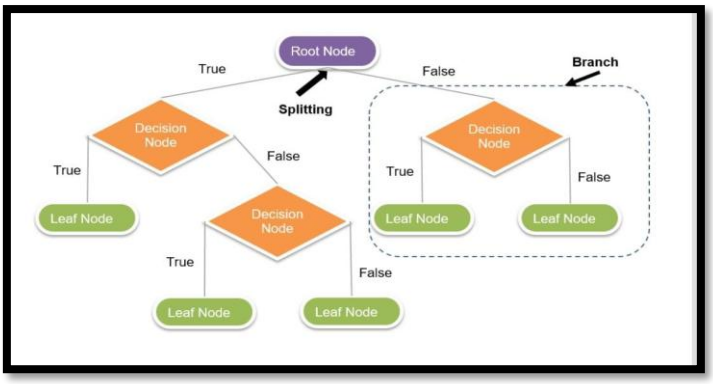
An NN structure consists of input nodes, many levels of hidden layers and output units that, via learning with every neuron receiving input and carrying out an action, enable self-optimization. The hidden layer receives output from the input after the input absorbs data from the external environment process. The hidden layer shapes it so that the output layer assigned to the external environment may accept and decipher it (Aderemi and Andronicus 2017). Introduced as a single layer with feed-forward and back-propagation NN, the hidden units were utilized random weights to provide output as input to the output layers (Talwar, A. and Kumar, Y. 2013). Normally, what are the NNs? While a neuron could not react as needed, the NNs also can learn and identify anomalies from categorized data patterns to get the appropriate result unlike conventional gradient-based algorithms which learn network weights slowly and rather rapidly. (Ziweritin, S., et al. 2022)



Source: Ziweritin, S., et al. 2022

1.4.2. Decision Tree

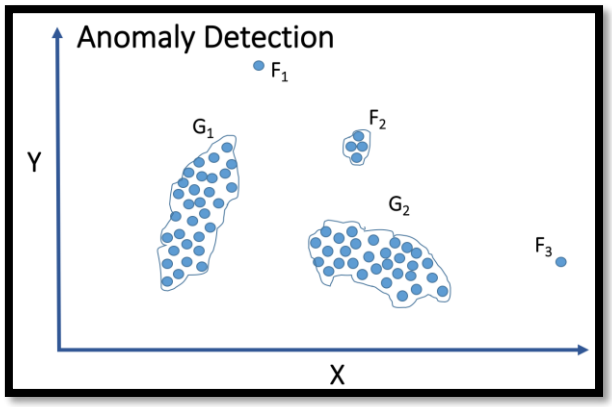
One of the most often used algorithms, a decision tree is a non-parametric supervised learning method whereby input is constantly split according to a predefined criterion. It develops inside the framework of a tree construction using if-then-else decision guidelines. Starting with a root node, a decision tree divides into several branches, links with other nodes, and so on. The result is a tree with decision and leaf nodes. Thus, this tactical approach of dividing and choosing helps the decision tree to simplify a complex problem. A decision tree's interpretability and fast extract insights from the modeling process flow by showing output visualization, therefore offering a major benefit. Besides, the decision tree is quick and requires little work in data preparation and data scaling. According to Sahin and Duman (2011), to handle fraud detection issues the decision tree model beats Support Vector Machine (SVM). If a tiny sample is utilized, the decision tree is simple to overfit however.



Source: Ziweritin, S., et al. 2022

1.4.3 Anomaly Detection

In machine learning, anomaly detection is a subfield where it is necessary to find the data samples that seem to be deviant of the typical properties of the dataset. Among these kinds of issues, defect detection in manufacturing, network intrusion detection, credit account fraud detection, etc. abound. Under anomalous conditions, in all these cases, a particular activity shows a significant rise or reduction that is reflected in the related characteristic of a multivariate test sample. Finding the aberrant activity and marking the sample as such is the ultimate aim. Unsupervised, supervised, and semi-supervised anomaly detection comprises three types of anomaly detection of which supervised anomaly detection is one.



Source: https://thecleverprogrammer.com/2020/11/04/what-is-anomaly-detection-in-machine-learning/

1.5 Significance of the Study

Safeguarding financial transactions is essential to maintaining customer confidence and economic stability given the growing acceptance of digital payments. This study will assist fintech start-ups, legislators, and financial institutions in better understanding the main cybersecurity concerns in digital payments and investigate how data science methods (such as blockchain security, anomaly detection, and AI-driven fraud detection) could help to lower risks. The results will offer practical ideas for strengthening regulatory compliance in digital banking, upgrading security systems, and boosting fraud avoidance techniques.

2. REVIEW OF LITERATURE:

2.1 **Ma, Y. (2025).** attempted to create a cyber-situational awareness model for banking industry payment systems to handle cybersecurity concerns like data breaches, fraud, and hostile assaults. Incorporating data acquisition, processing, situational awareness, and reaction decision-making into the suggested model, the study showed, enhanced threat detection and response. It attained better applicability, shorter reaction times, and more accuracy by combining multi-source data and machine learning than by using current approaches The results supplied a technological and theoretical guide for improving payment system security.

2.2 **Lakshmi, R., & Rani, S. (2024)** aimed to identify threats to digital wallets, such as malware, data breaches, phishing, and contactless payment risks, and also proposed to provide countermeasures like regulatory compliances,

use of education and technological solutions to safeguard digital payment systems and also to enhance the security around it. The research revealed that because of their general acceptance, fraudsters are progressively focusing on digital wallets. Major concerns were phishing, malware, data leaks, and illegal access. By including encryption, multi-factor authentication, regulatory compliance, and user education—a multi-layered security strategy these risks were substantially lowered. Maintaining confidence and dependability in digital payment systems was also shown to depend critically on increasing user knowledge and implementing industry security standards.

2.3 **Kumar, S., & Bansal, G. (2024).** focused on developing issues such assaults on vital infrastructure, data breaches, and vulnerabilities in the expanding digital payment systems, thereby analyzing the cybersecurity concerns inherent in India's path of digital transformation. The research emphasizes how urgently a strong cybersecurity infrastructure and regulatory set are needed. The results support a multi-stakeholder strategy including government, businesses, and people to guarantee India's digital future while preserving the speed of innovation and inclusiveness.

2.4 **Gupta, R. (2024).** examined phishing, malware, data breaches, and insider threats among cybersecurity risks compromising e-commerce systems. It also looked at newly developing themes such IoT vulnerabilities, AI-driven cyberattacks, and the impact of legislative developments. It was found that e-commerce sites deal with ever more complex cyber risks as IoT and artificial intelligence widen the attack ground. Among the effective countermeasures were encryption, safe payment gateways, intrusion detection systems, staff training, and regulatory compliance that is, GDPR, CCPA. Strengthening cybersecurity also depends critically on industry collaboration and information exchange. The results underlined the need of a proactive, multi-layered strategy combining legal adherence to protect e-commerce activities, adaptive security techniques, and constant monitoring.

2.5 **Roy, A., & Sarker Tinny, S. (2024)** examined how effectively blockchain technology and cybersecurity may reduce cyber threats, hence improving the security of digital payments. The findings indicated that, blockchain guarantees decentralization, immutability, and openness, thereby enhancing the security of digital payments. Several cybersecurity systems were found to be necessary in threat prevention. Although blockchain and cybersecurity help to improve payment security, there are possible hazards that need for smart deployment. The results gave legislators and financial organizations new ideas on protecting digital financial transactions.

2.6 **Sunderajulu, K. B. (2024)** investigated security systems in digital payment transactions, evaluated industry norms and regulations, and looked at potential developments to help to reduce cybercrime and fraud. While tokenization, conformity with regulatory requirements, and safe cryptographic methods improve payment security, the study revealed that new technologies present new difficulties even in this regard. Mobile wallets, contactless payments, and eCommerce transactions taken together need for flexible security systems. Future developments will center on enhanced cryptographic algorithms to ensure transaction security and preserve customer confidence, AI-driven fraud detection, and better interoperability.

2.7 **Sharma, H. P., et al. (2023)** investigated security flaws, looked at the development of electronic payment systems, and suggested fixes to improve their dependability for expansion of e-business. The findings indicated that even if e-payment systems have developed to provide convenience, fast developing cyber-attack strategies cause security flaws even in these systems. It underlined the dearth of sufficient security mechanisms and proposed changes to create a more reliable e-payment system. Examining questionable purchase rates gave information needed to create more dependable and safe electronic payment systems.

2.8 **Sarker, I. H. (2023).** investigated how machine learning may be used for proactive threat detection, intelligent data analysis, and automation in cybersecurity. The paper concluded that machine learning greatly improves cybersecurity by allowing automated and data-driven threat detection, Different machine learning approaches enhance security intelligence using proactive defence above conventional approaches. The research also pointed out important issues including data quality and algorithm efficiency as well as suggested future options for besting cybersecurity solutions.

2.9 **Saeed, S., et al. (2023)** investigated how digital transformation (DT) may affect cybersecurity as well as how it might help to attain corporate resilience According to the report, DT raises cybersecurity threats like data breaches and cyberattacks even when it improves efficiency and output. Major risks and weaknesses companies encounter during DT deployment were found by a thorough literature study applying the PRISMA approach. The paper emphasizes the need of a cybersecurity ready architecture to reduce risks and guarantee the defence of digital resources.

2.10 **Chang, V., et al (2022)** assessed many machine learning techniques using actual credit card transaction data to find an effective and steady fraud detection model for Industry 4.0. Among the five models evaluated, random

forest and logistic regression came out as performing best according to the research. Using principal component analysis and under sampling further enhanced fraud detection accuracy. The paper emphasizes how well feature selection and sample techniques improve fraud detection in the digital economy and Industry 4.0.

2.11 **Ziweritin, S., et al. (2022).** investigated outcome abnormalities in student evaluations using a comparison between neural network and decision tree models. The decision tree model attained 91%; the feed-forward multi-layered neural network attained 96% accuracy. Weight addition and calibrated values raised model intelligence and classification accuracy.

2.12 **Sarker, I. H., et al. (2020)** investigated using machine learning methods, security event pattern analysis, and automated security solution development the function of data science in cybersecurity. By using machine learning-based multi-layered systems, cybersecurity data science improves security intelligence, the study revealed. Data-driven insights enhance threat detection and response, hence enabling more flexible security solutions.

3. OBJECTIVES OF THE STUDY:

1. To analyse cybersecurity threats in digital payment systems (DPS).

2. To study the role of data science techniques in threat detection and prevention.

4. RESEARCH METHODOLOGY:

This exploratory study utilizes a survey-based questionnaire to get the primary data, while secondary data was used to review past literatures. The sample size is 392 fintech users, chosen using convenience sampling. Descriptive research is performed using Exploratory Factor Analysis (EFA) by utilizing SPSS.

5. DATA ANALYSIS AND INTERPRETATION:

Table No: 1 Descriptive Statistics

	Mean	Std. Deviation	Analysis N
Phishing Attacks	4.70	.460	392
Account Takeover (ATO)	4.27	.814	392
Card Skimming	4.68	.504	392
SIM Swapping Fraud	4.34	.740	392
Deepfake & Social Engineering Attacks	4.32	.869	392
Unauthorized Access to Payment Data	3.41	1.015	392
Malware & Keyloggers	3.34	.988	392
Ransomware Attacks	3.21	1.066	392
Weak Encryption Protocols	3.21	1.099	392
Insecure Mobile Wallets & Apps	3.36	1.027	392
Man-in-the-Middle (MITM) Attacks	3.45	1.018	392
Public Wi-Fi Exploits	3.14	1.044	392
DDoS Attacks on Payment Gateways	3.55	1.035	392
API Security Vulnerabilities	3.45	1.086	392
Outdated Software & System Exploits	3.59	1.132	392

The results demonstrate considerable apprehension around phishing attacks (4.70) and card skimming (4.68), although threats such as SIM switching (4.34) and deepfake assaults (4.32) also present notable concerns. System vulnerabilities, including inadequate encryption (3.21) and unsecured mobile wallets (3.36), present moderate concern. Elevated standard deviations in certain domains indicate diverse perspectives. Fortifying security protocols is vital to augment the safety of digital payments.

Table No: 2 KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.759
Bartlett's Test of Sphericity	Approx. Chi-Square	5329.626
	df	105
	Sig.	.000

Based on the preceding table, one may deduce that the data is suitable for more investigation as value of KMO =.759 shows that the current data has sufficient sample. Furthermore, value of Bartlett's test =.000 shows that the correlation matrix differs from the identity matrix and sufficient correlation exists between the variable.

Table No: 3 Communalities		
	Initial	Extraction
Phishing Attacks	1.000	.584
Account Takeover (ATO)	1.000	.510
Card Skimming	1.000	.800
SIM Swapping Fraud	1.000	.442
Deepfake & Social Engineering Attacks	1.000	.406
Unauthorized Access to Payment Data	1.000	.829
Malware & Keyloggers	1.000	.897
Ransomware Attacks	1.000	.849
Weak Encryption Protocols	1.000	.870
Insecure Mobile Wallets & Apps	1.000	.830
Man-in-the-Middle (MITM) Attacks	1.000	.626
Public Wi-Fi Exploits	1.000	.663
DDoS Attacks on Payment Gateways	1.000	.671
API Security Vulnerabilities	1.000	.920
Outdated Software & System Exploits	1.000	.831
Extraction Method: Principal Component Analysis.		

According to the above table, every value of the communalities of the objects falls between 0.534 until 0.871, over the cut condition of 0.50. Sum of square of factor loading horizontally are communalities. Average correlation between the objects is communality.

Table No: 4 Total Variance Explained									
Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	5.984	39.895	39.895	5.984	39.895	39.895	4.602	30.683	30.683
2	2.600	17.332	57.228	2.600	17.332	57.228	3.603	24.023	54.706

3	2.143	14.284	71.512	2.143	14.284	71.512	2.521	16.805	71.512
4	.970	6.468	77.979						
5	.796	5.309	83.288						
6	.611	4.073	87.361						
7	.446	2.971	90.332						
8	.397	2.644	92.976						
9	.267	1.777	94.753						
10	.251	1.676	96.429						
11	.213	1.418	97.847						
12	.159	1.063	98.910						
13	.067	.450	99.359						
14	.052	.344	99.703						
15	.045	.297	100.000						
Extraction Method: Principal Component Analysis.									

As seen above table column **EIGENVALUE** shows sum of square of factor loading vertically and all the factors retaining eigenvalue value larger than 1 are kept. First three factors therefore have eigenvalue of 5.984, 2.600, and 2.143 hence all three factors are kept.
The eigenvalues are shown in Column **TOTAL**. It may be claimed that all the following factors will extract less variance than the current factor since the first factor accounts maximal variation and the succeeding factors will include left-over variation. Column **PERCENTAGE** OF VARIANCE shows each factor's explained proportion of variance. Eigenvalue/total items times 100 is what I mean. Column **CUMULATIVE PERCENTAGE** shows total of variations explained by all the previous and current elements. The three elements taken overall show 71.512.

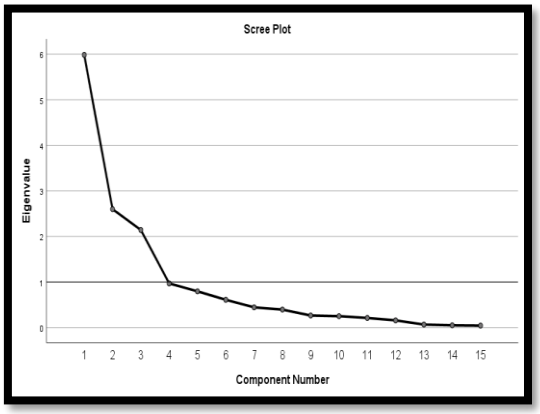


Figure No: 2 Scree Plot

According to figure no.2, the number of factors that can be kept is ascertained. Cattell (1966) claims that all the elements causing the largest variation in the data set are removed; the eigenvalues are shown on the y-axis and the number of components that might be obtained on the x-axis. Eigenvalue is the sum of the factor loadings of the vertically rotated component matrix; all the factors with Eigenvalue are obtained. Consequently, it is clear that three elements have eigenvalues higher than 1; the form of the curve becomes homogeneous after the fourth component. The Scree test shows then that all three requirements can be maintained.

Table No:5 Rotated Component Matrix	

	Data Breach & Privacy Threats	Network & System Vulnerabilities	Fraud & Identity Theft Threats
Phishing Attacks – Receiving fake emails/messages to steal financial credentials.			.762
Account Takeover (ATO) – Hackers gaining unauthorized access to user accounts.			.593
Card Skimming – Cloning debit/credit cards at ATMs or POS terminals.			.894
SIM Swapping Fraud – Fraudsters hijacking mobile numbers to reset banking passwords.			.585
Deepfake & Social Engineering Attacks – AI-generated voice/video scams tricking users.			.612
Unauthorized Access to Payment Data – Hackers breaching financial databases.	.884		
Malware & Keyloggers – Malicious software recording keystrokes to steal banking info.	.922		
Ransomware Attacks – Hackers encrypting financial data and demanding payment.	.891		
Weak Encryption Protocols – Vulnerabilities in financial data encryption.	.908		
Insecure Mobile Wallets & Apps – Payment apps storing user data without proper security.	.892		
Man-in-the-Middle (MITM) Attacks – Hackers intercepting transactions on unsecured networks.		.697	
Public Wi-Fi Exploits – Data theft when users make payments on unsecured networks.		.758	
DDoS Attacks on Payment Gateways – Hackers disrupting banking servers.		.806	
API Security Vulnerabilities – Weak security in third-party payment integrations.		.935	
Outdated Software & System Exploits – Cybercriminals exploiting unpatched banking systems.		.885	

As per above table, rotated component matrix there are 5 variables in factor 1, there are 5 variables in factor 2 and there are 5 variables in factor 3. Rotated component matrix table gives the correlation between the variables and the dimension. The values of component matrix are known as factor loading. These are the correlation values; hence, possible values range from – 1 to +1. So, it is seen that total 10 items have clubbed and formed 3 independent factors and are named as Data Breach & Privacy Threats, Network & System Vulnerabilities, and Fraud & Identity Theft Threats.

6. RESULTS AND DISCUSSION:

The study underscores significant cybersecurity concerns impacting digital payment systems, highlighting the weaknesses present in financial data protection, network security, and fraud prevention. Data breaches and privacy issues present considerable hazards stemming from illegal access, malware, ransomware, inadequate encryption, and unsecured mobile applications. These weaknesses expose financial organizations and consumers to possible losses

and identity theft, needing enhanced security standards and sophisticated encryption technologies. Similarly, deficiencies in network and system security, including unprotected public networks, obsolete software, and API vulnerabilities, create opportunities for hackers to track transactions and destabilize payment systems. Mitigating these attacks necessitates strong security frameworks, prompt software upgrades, and improved monitoring systems to identify anomalies in real time.

Persistent advancement of fraud and identity theft using complex techniques including phishing, account takeovers, card skimming, and deepfake scams is attributed to These risks increase the frequency and obscurity of financial fraud by using system weaknesses and user confidence. To lower cyber risks, the study emphasizes the need of using multi-layered authentication, artificial intelligence-based fraud detection, and user education programs. Maintaining consumer confidence and enabling the continuous financial transaction execution depend on improving cybersecurity in digital payment systems. Future research should look at adaptive security systems combining blockchain and artificial intelligence to effectively reduce emerging cyber risks.

Financial institutions should give the implementation of modern encryption protocols, AI-powered fraud detection, and biometric authentication priority which can help in improving cybersecurity in digital payment systems. Strict industry standard compliance, regular software upgrades, and frequency of security audits help to reduce data breaches and system vulnerabilities related to risks. Reducing deceptive conduct also depends on raising user knowledge of cyber dangers, phishing scams, and safe payment methods employing financial literacy programs. Developing evolving security systems that can efficiently fight changing cyber threats depends on cooperation among authorities, technological companies, and financial institutions.

REFERENCES:

[1] Aderemi, O.A. and Andronicus, A.A. (2017) A Survey of Machine-Learning and Nature-Inspired Based Credit Card Fraud Detection Techniques. International Journal of System Assurance Engineering and Management, 8, 937-953. https://doi.org/10.1007/s13198-016-0551-y

[2] Aftergood, S. (2017). Cybersecurity: The cold war online. Nature, 547(7661),. https://doi.org/10.1038/547030a

[3] Al-Laham, M., Al-Tarawneh, H., & Abdallat, N. (2009). Development of electronic money and its impact on the central bank role and monetary policy. Issues in Informing Science and Information Technology, 6, 339-349.

[4] Cao, L. (2017). Data science: Challenges and directions. Communications of the ACM, 60(8), 59–68. https://doi.org/10.1145/3076253

[5] Chang, V., Di Stefano, A., Sun, Z., & Fortino, G. (2022). Digital payment fraud detection methods in digital ages and Industry 4.0. Computers and Electrical Engineering, 100, 107734.

[6] Cukier, K. (2010). Data, data everywhere: A special report on managing information. The Economist.

[7] Gupta, R. (2024). Cybersecurity Threats in E-Commerce: Trends and Mitigation Strategies. 1(3), 1–10. https://doi.org/10.36676/jams.v1.i3.13

[8] Hey, A. J., Tansley, S., & Tolle, K. M. (Eds.). (2009). The fourth paradigm: Data-intensive scientific discovery. Microsoft Research.

[9] Khando, K., Islam, M. S., & Gao, S. (2022). The emerging technologies of digital payments and associated challenges: A systematic literature review. Retrieved from https://www.mdpi.com/1999-5903/15/1/21#metrics

[10] Kumar, S., & Bansal, G. (2024). Digital vulnerabilities: cybersecurity threats in india's digital transformation journey. ShodhKosh Journal of Visual and Performing Arts, 5(1). https://doi.org/10.29121/shodhkosh.v5.i1.2024.3726

[11] Lakshmi, R., & Rani, S. (2024). Securing digital wallets: threats and countermeasures. mLAC Journal for Arts Commerce and Sciences (m-JACS), 2(4), 25–32. https://doi.org/10.59415/mjacs.v2i4.185

[12] Ma, Y. (2025). Research on Security Situation Awareness Model Based on Financial Industry Payment Scenario. Financial Economics Insights., 2(1), 1–11. https://doi.org/10.70088/qsyq6j57

[13] Pirani, S. (2024). Navigating Research Ethics: Strategies for preventing and Addressing Research Misconduct, International Journal of Multidisciplinary Research & Reviews, Vol 03, No. 02, PP.96-104.

[14] Pirani, S. (2024). Simplifying statistical Decision Making: A Research Scholar's Guide to parametric and Non-Parametric Methods, International Journal of Multidisciplinary Research & Reviews, Vol 03, No. 03, pp. 184-192.

[15] Roy, A., & Sarker Tinny, S. (2024). Cybersecurity and Blockchain for Secure Financial Transactions: Evaluating, Implementing, and Mitigating Risks of Digital Payments. International Journal of Applied and Natural Sciences, 1(2), 38–48. https://doi.org/10.61424/ijans.v1i2.95
[16] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666.
[17] Şahin, Y. G., & Duman, E. (2011). Detecting credit card fraud by decision trees and support vector machines. In Proceedings of the International MultiConference of Engineers and Computer Scientists 2011.
[18] Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. Annals of Data Science, 10(6), 1473-1498.
[19] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 7, 1-29.
[20] Saxe, J., & Sanders, H. (2018). Malware data science: Attack detection and attribution. No Starch Press.
[21] Sharma, H. P., Krishna, S. H., R., V., Tiwari, M., Tiwari, T., & Kumar, M. N. (2023). Analysis of Cyber Security Threats in Payment Gateway Technology. https://doi.org/10.1109/icacite57410.2023.10183063
[22] Sule, M. J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: issues and trends. Technology in Society, 67, 101734.
[23] Sunderajulu, K. B. (2024). Enhancing Payment Transaction Security. International Journal of Science and Research, 13(11), 680–684. https://doi.org/10.21275/sr241110202744
[24] Talwar, A. and Kumar, Y. (2013) Machine Learning: An Artificial Intelligence Methodology. International Journal of Engineering and Computer Science, 2, 3400-3404.
[25] Ziweritin, S., Baridam, B.B. and Okengwu, U.A. (2022) A Comparative Analysis of Neural Network and Decision Tree Model for Detecting Result Anomalies. Open Access Library Journal, 9, 1-15. doi: 10.4236/oalib.1108549.
[26] V. Yamuna;Praveen RVS;R. Sathya;M. Dhivva;R. Lidiya;P. Sowmiya, “Integrating AI for Improved Brain Tumor Detection and Classification” 2024 4th International Conference on Sustainable Expert Systems (ICSES), DOI: 10.1109/ICSES63445.2024.10763262
[27] Sarthak Sharma;Suman Vij;RVS Praveen;S. Srinivasan;Dharmendra Kumar Yadav;Raj Kumar V S, “Stress Prediction in Higher Education Students Using Psychometric Assessments and AOA-CNN-XGBoost Models,” 2024 4th International Conference on Sustainable Expert Systems (ICSES), DOI: 10.1109/ICSES63445.2024.10763288
[28] Dr. Swapnil B. Mohod, Ketki R. Ingole, Dr. Chethana C, Dr. RVS Praveen, A. Deepak, Mrs B. Sukshma, Dr. Anurag Shrivastava."Using Convolutional Neural Networks for Accurate Medical Image Analysis", 3819-3829, DOI: https://doi.org/10.52783/fhi.351
[29] Dr. Mohammad Ahmar Khan, Dr. Shanthi Kumaraguru, Dr. RVS Praveen, Narender Chinthamu, Dr Rashel Sarkar, Nilakshi Deka, Dr. Anurag Shrivastava, "Exploring the Role of Artificial Intelligence in Personalized Healthcare: From Predictive Diagnostics to Tailored Treatment Plans", 2786-2798, DOI: https://doi.org/10.52783/fhi.262
[30] B. Sangeetha, RVS Praveen, K. Sivakumar, Deshmukh Narendra Pandurang, Deepak Sundrani, K. Soujanya. (2024). Behavioural Economics and Consumer Decision-Making: A Study of Financial Products. European Economic Letters (EEL), 14(3), 2441–2450.
[31] Devyani Chatterji, Raghvendra, RVS Praveen, Chaitanya Koneti, Sumi Alex, Deeja S. (2024). Challenge and Impact and Role of Innovation and Entrepreneurship in Business Growth. European Economic Letters (EEL), 14(3), 1141–1149. https://doi.org/10.52783/eel.v14i3.1875
[32] Sandeep Lopez ,Dr. Vani Sarada ,Dr. RVS Praveen, Anita Pandey ,Monalisa Khuntia, Dr Bhadrappa Haralayya, "Artificial Intelligence Challenges and Role for Sustainable Education in India: Problems and Prospects", Vol. 44 No. 3 (2024): LIB PRO. 44(3), JUL-DEC 2024 (Published: 31-07-2024), DOI: https://doi.org/10.48165/bapas.2024.44.2.1
[33] Shrivastava, A., Chakkaravarthy, M., Shah, M.A..A Novel Approach Using Learning Algorithm for Parkinson’s Disease Detection with Handwritten Sketches. In Cybernetics and Systems, 2022
[34] Shrivastava, A., Chakkaravarthy, M., Shah, M.A., A new machine learning method for predicting systolic and diastolic blood pressure using clinical characteristics. In *Healthcare Analytics*, 2023, 4, 100219

[35] Shrivastava, A., Chakkaravarthy, M., Shah, M.A.,Health Monitoring based Cognitive IoT using Fast Machine Learning Technique. In *International Journal of Intelligent Systems and Applications in Engineering*, 2023, 11(6s), pp. 720–729

[36] Shrivastava, A., Rajput, N., Rajesh, P., Swarnalatha, S.R., IoT-Based Label Distribution Learning Mechanism for Autism Spectrum Disorder for Healthcare Application. In *Practical Artificial Intelligence for Internet of Medical Things: Emerging Trends, Issues, and Challenges*, 2023, pp. 305–321

[37] Shrivastava, A., Pundir, S., Sharma, A., ...Kumar, R., Khan, A.K. Control of A Virtual System with Hand Gestures. In *Proceedings - 2023 3rd International Conference on Pervasive Computing and Social Networking, ICPCSN 2023,* 2023, pp. 1716–1721

[38] Sheela Hhundekari, Advances in Crowd Counting and Density Estimation Using Convolutional Neural Networks, International Journal of Intelligent Systems and Applications in Engineering, Volume 12, Issue no. 6s (2024) Pages 707–719

[39] Kamal Upreti, Prashant Vats, Gauri Borkhade, Ranjana Dinkar Raut, Sheela Hundekari, Jyoti Parashar, An IoHT System Utilizing Smart Contracts for Machine Learning -Based Authentication, 2023 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), 10.1109/ETNCC59188.2023.10284960

[40] S Gupta, N Singhal, S Hundekari, K Upreti, A Gautam, P Kumar, R Verma, Aspect Based Feature Extraction in Sentiment Analysis using Bi-GRU-LSTM Model, Journal of Mobile Multimedia, 935-960

[41] PR Kshirsagar, K Upreti, VS Kushwah, S Hundekari, D Jain, AK Pandey, Prediction and modeling of mechanical properties of concrete modified with ceramic waste using artificial neural network and regression model, Signal, Image and Video Processing, 1-15

[42] ST Siddiqui, H Khan, MI Alam, K Upreti, S Panwar, S Hundekari, A Systematic Review of the Future of Education in Perspective of Block Chain, Journal of Mobile Multimedia, 1221-1254

[43] Kamal Upreti, Anmol Kapoor, Sheela Hundekari,Deep Dive Into Diabetic Retinopathy Identification: A Deep Learning Approach with Blood Vessel Segmentation and Lesion Detection, 2024: Vol 20 Iss 2, https://doi.org/10.13052/jmm1550-4646.20210

[44] Ramesh Chandra Poonia; Kamal Upreti; Sheela Hundekari; Priyanka Dadhich; Khushboo Malik; Anmol Kapoor, An Improved Image Up-Scaling Technique using Optimize Filter and Iterative Gradient Method, 2023 3rd International Conference on Mobile Networks and Wireless Communications (ICMNWC) ,04-05 December 2023, 10.1109/ICMNWC60182.2023.10435962

[45] Venata Sai Chandra Prasanth Narisetty and Tejaswi Maddineni, Revolutionizing Mobility: The Latest Advancements in Autonomous Vehicle Technology, Nanotechnology Perceptions, 20 No. S12(2024),1354–1367.

[46] Venata Sai Chandra Prasanth Narisetty and Tejaswi Maddineni,Powering the Future: Innovations in Electric Vehicle Battery Recycling, Nanotechnology Perceptions 20 No. S13 (2024) 2338-2351.