International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
IJISAE
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Innovation Detection of Vulnerabilities for Digital Transactions in Financial Institutions Using Cyber Security Framework

Dr. R. Sangeetha[1], Dr. R. Priscilla Joy*[2], M. Denisha [3], Dr. Julia Punitha Malar Dhas

Submitted: 20/04/2023 **Revised**: 22/06/2023 **Accepted**: 03/07/2023

Abstract: Cyber security is an important and growing challenge in the world today. As technology advances, so do the potential threats posed by malicious actors. Cyber security is the practice of protecting networks, systems, and programs from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes. Cyber security threats come from a variety of sources, including activists, criminals, fo reign governments, and terrorists. All of these actors are constantly developing new tools and techniques for attacking systems. As a result, organizations must stay on top of the latest developments in order to protect themselves from these threats. One of the biggest challenges in cyber security is defending against the ever-evolving threats posed by malicious actors. To do this, organizations must have a comprehensive security strategy in place. In this paper, a cyber-security framework has proposed to identify the cyber threats. This strategy should include preventative measures such as firewalls, monitoring systems, and patch management. It should also include detection and response measures, such as incident response plans and digital forensics. Another challenge is staying ahead of the attackers. Attackers are constantly using new techniques and tools, making it difficult to defend against them. Organizations must stay up-to-date with the latest.

Keywords: *Cyber security, Digital attacks, Sensitive information, Hacking, Framework*

1. Introduction

As technology keeps changing, there is a shortage of qualified people [1]. Due to digital transformation, it is necessary to provide skill development training to the employees and bridge the skill gap [2]. A prepared, future-proof workforce can only prevent a cyber attack. Therefore, companies should adopt modern cyber security measures and strengthen their team with employees who have advanced skills in cyber security [3-4]. An average annual cost of Rs. 75 crores in economic loss. A recent study revealed that this loss occurs both directly and indirectly [5]. The report also pointed out that cyber-attacks are causing micro-economic impacts including loss of jobs [6]. The direct loss in India is only $90,000. But the loss due to reasons including loss of jobs and loss of confidence in the company is 31 lakh dollars. Similarly, the cost of microeconomic impacts, i.e. reduced customer base and cost to companies, is estimated at 63 lakh dollars [7-8]. Microsoft and Prost & Sullivan jointly conducted a study on the impact of cyber attacks in the Asia Pacific region [9]. It has mentioned that the loss due to cyber attack for medium-sized companies is 11 thousand dollars [10]. The study was conducted among more than 1,300 IT companies and mid-sized companies [11]. The study was conducted in a total of 13 Asia Pacific countries [12]. The network security model has shown in the following fig.1

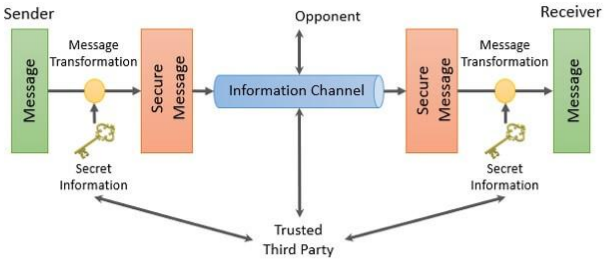

Fig 1: Networks security model

The impact in the manufacturing sector is estimated to be 18 percent and the impact in the financial sector is 12 percent. It is also estimated that 11 percent of cyber attacks are carried out in government institutions [13]. The study revealed that nearly 62 percent of companies in India have been cyber-attacked [14]. However, only 38 percent of organizations regularly evaluate

and report data breaches [15]. Cyber attacks are a major topic of discussion for organizations transitioning to digital [16]. But most companies don't pay enough attention to cyber attacks. Only 20 percent of organizations prioritize cyber-attacks from the start [17]. Actions taken after a cyber attack are less effective than preventive measures. But more than 50 security solutions are the best sellers [18-19]. Artificial intelligence technology and cyber security measures all help to counter cyber attacks and prevent this threat, the study suggests [20]. Cyber Attack It can be any

1 Karunya Institute of Technology and Sciences, Coimbatore
ORCID ID : 0000-0003-2708-231X
2 Karunya Institute of Technology and Sciences, Coimbatore
ORCID ID : 0000-0001-5778-8415
3 Karunya Institute of Technology and Sciences, Coimbatore
ORCID ID : 0000-0001-5870-2943
4 Karunya Institute of Technology and Sciences, Coimbatore
ORCID ID : 0000-0003-3904-1902
Corresponding author: rpj.joy@gmail.com

activity carried out on a computer or on a mobile or desktop device such as computers and is carried out by a group of people who have extensive knowledge of computers and computing [21]. There are many types of cyber attacks [22]. A 'system key' has been found that can unlock files that have been hacked by a cyber attack [23]. Ransom ware is dangerous software that can steal data from a

computer [24-25]. Also worth making files unusable. After the attack through this, the hackers will ask for money to release these hacked files [26]. We send money to someone without much hassle through UPI transaction apps [27]. But as easy as it is, it needs to be handled carefully. Google Pay, Paytm, Phone Pay, WhatsApp Pay etc. are widely used nowadays [28]. Similarly many other new apps are going to be introduced in the market considering the demand [29]. So it is important to know which apps to use and which to avoid [30].

Digital attacks in financial institutions are a growing issue. Cyber criminals are taking advantage of the evolution of technology and are increasingly targeting banks, financial institutions, and even individual customers [31]. These attacks can range from simple phishing attempts to sophisticated malware and ransom ware attacks. The goal of these attacks is often to gain access to confidential customer data and financial information [32]. The attackers may be looking to access customer accounts, steal money, or gain access to sensitive data like credit card numbers or passwords. Financial institutions are particularly vulnerable to cyber-attacks because they store and process large amounts of sensitive data and have access to multiple customer accounts [33].

2. Related Works

Digital cyber attacks are a reality of the modern world. They are a form of cybercrime, which is the use of technology to commit crimes or cause harm to individuals, businesses, or government institutions. Cyber attacks are conducted with malicious intent, and can range from stealing sensitive data and financial information to disrupting services and networks [4]. Digital cyber attacks can take many forms, from phishing emails to ransom ware, malicious software, and other forms of malicious code. In some cases, they can be used to gain access to confidential data or networks, or to sabotage a company’s operations [6]. They can also be used to extort money or disrupt services. The best way to protect against digital cyber attacks is to take preventive measures such as installing up-to-date anti-virus and firewall software. It is also important to have strong passwords and use two-factor authentication whenever possible [7]. Additionally, organizations should regularly monitor their networks for potential vulnerabilities and take steps to patch any discovered weaknesses. Organizations should also take steps to educate their employees on how to identify and respond to cyber threats [9]. This includes training on the signs of a phishing email, installing software patches, and establishing strong security policies. Additionally, companies should have a plan in place for responding [11].

The incidence of cyber attacks and cyber breaches has increased in various sectors. Since the pandemic, the trend has intensified with many working from home. This is also due to increased digitization and rise in online transactions [16]. A recent report by the Information Systems Security Association points to this trend. The report suggests that cyber attacks have increased by 63 percent internationally during the pandemic. Covid-19 favors fraudsters, hackers [17]. With the increasing number of attacks, it is becoming imperative for organizations worldwide to employ staff capable of preventing attacks. While the use of modern technologies such as AI, ML, and increasing automation are the reasons for the increase in cyber attacks, the lack of professional staff capable of understanding such modern technologies is also a reason [20]. A study conducted by the international non-profit organization ISC suggests that cyber security staff have been outsourced to other IT tasks in this era. It is a fact that data leakage and cyber attacks are on the rise [23]. Cyber attack methods are also changing in the context of digitization and increase in digital transactions. In this situation, the key question arises as to how companies can cope with this challenge amid a shortage of skilled workers. Dealing with these attacks requires the right devices and partners [25]. It is essential to build secure infrastructure. It is necessary to carry out frequent inspections in conjunction with qualified persons to identify gaps. As far as organizations are concerned, employees are the weakest link [27]. With so many different types of attacks taking place, it is imperative to focus on cyber security awareness. In 2021, one in 61 organizations worldwide will be the target of a cyber attack. However, they warn that data leakage and cyber attacks due to digitization will increase in the coming times [30].

I. Proposed Model

Each of the malware types has a reputation for displaying a subtle villainy. Ransom ware malware is a very common malware package. In today's global cybercrime, many companies fall victim to ransom ware attacks. Day by day the cyber attacks carried out with this ransom ware are increasing. It's as if Saturn has been lifted and put in the banyan. So I have no doubt that if each one of us is very vigilant, we can protect our hard-earned wealth and our company's assets and reputation from this digital thief called ransom ware. The proposed model block diagram has shown in the following fig.2

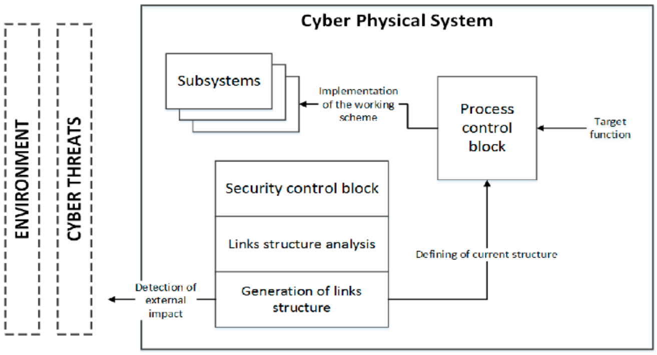

Fig 2: Proposed model block diagram

Cyber Security threats

Majority of global business organizations and government organizations are today the target of constant attacks by cybercriminals. Important malwares are listed below.

- Spyware
- Advertisement Ware
- Trojan
- Click Logger
- Ransom ware
- Bots

The weapons these cybercriminals use in their attacks are software programs written for malicious purposes known as malware. Today, various types of malware are developed and used by cybercriminals to fulfill their various objectives. In the form of phishing links, they create a fake third-party website for financial fraud. The website thus created can be a replica of a popular bank or a popular e-commerce company's website. By sending the links of such created website to the customers through SMS or social networking sites, the banks will get the relevant personal information from the customer. This will lead to financial fraud. Avoid clicking on unfamiliar, unverified links. If you receive any unsolicited website links via SMS or email, delete them immediately. Financial fraudsters trick customers into downloading screen sharing apps with fake website links. Then the customer's mobile phone or laptop screen is shared through the screen sharing app and the financial transaction information shared on it is stolen.

Issues in Cyber threats

Ransom ware malware is a very common malware package. In today's global cybercrime, many companies fall victim to ransom ware attacks. After a cyber attack on a company, a hacker expects a large amount of money (Ransom) from the company to prevent the public release of the company's most sensitive data that he has captured and to decrypt the company's encrypted data, then it is a ransom ware malware attack. known as The number of successful ransom ware attacks worldwide is increasing dramatically. The amount of money paid by companies affected by ransom ware attacks to these hackers is also increasing exponentially.

Thereby financial fraud takes place. In case customers are asked to download a screen sharing app to deal with any technical glitch on their devices, they should first delete the Internet Banking transaction information from other transaction apps on the devices. After using an app related to screen sharing app, you should remove it from the devices. Financial fraudsters use skimming devices in ATM machines to steal customers' ATM card information. With such stolen information, financial fraud can be carried out with fake ATM cards, or fraudsters pose as other customers near ATM machines that customers can use, track ATM passwords, and then engage in financial fraud. Are there any additional machines used in the particular Make sure that. Customers should hide their ATM passwords from others when they enter them. Customers using ATM machines should avoid using passwords in the presence of unknown persons in their vicinity.

Security Actions

Daily and weekly all important information of your company and backups should be maintained at a secure location. Fortify company's servers and desktops with antivirus and antimalware security programs. Completely ban the use of flash drives on your company's servers and desktops. The Access Privileges for Servers and Desktops should be scrutinized and regulated on an only in Need to Know Basis. Passwords and security controls of servers and desktops should be made stricter. Immediately remove and isolate servers and desktops affected by ransom ware attacks from the company network. Organizations should establish a full-time security operation center to continuously monitor cyber attack attempts by various malwares like ransom ware on the organization and take appropriate precautionary measures. Carefully collect the digital footprints created by ransom ware malware to inform important policy decisions about the company's next level of cyber security. Every large business should take a cyber insurance policy. Periodically sensitize employees about email-borne ransom ware and other malware attacks.

3. Results and Discussion

The proposed cyber security framework (CSF) has compared with the existing Secured Database Monitoring Method (SDMM) and Multi-Factor Authentication Method (MFAM).

Multi-factor authentication

It can also make the app you use more secure by selecting certain features. Multi Factor Authentication allows you to receive OTP to mobile or email instead of just using user ID and password. After typing the OTP correctly, the app will display the correct information. So keep this feature turned on. Keep the facility of receiving notification whenever payment is made or withdrawn in your bank account. The comparison of multifactor authentication has shown in the following table 1.

Table 1: Comparison of multi-factor authentication

Inputs	SDMM	MFAM	CSF
100	62.77	87.21	92.58
200	61.72	86.20	91.44
300	60.67	85.19	90.30
400	59.62	84.18	89.16
500	58.57	83.17	88.02

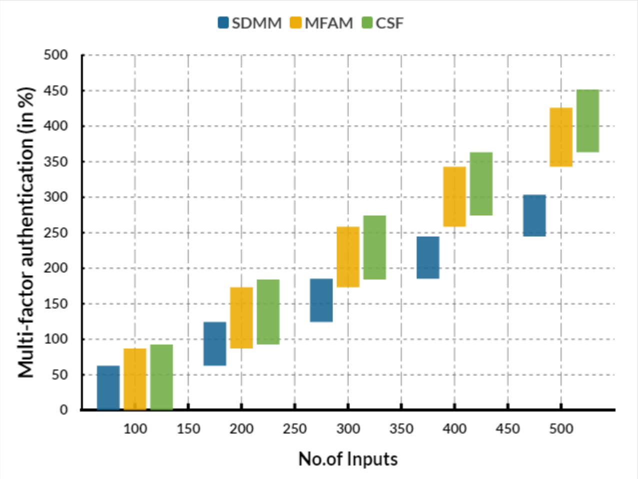

Fig.3: Comparison of multi-factor authentication

The fig.3 shows the comparison of multi-factor authentication. It can add SMS and email notification facility. If you receive SMS about your bank balance, read it and delete it after a couple of days. If someone steals your phone or you forget to lock your phone, other people can find out your bank balance. Financial fraudsters often force customers to use some form of QR code scan. By doing so, they get permission to make transactions from the customers' bank accounts. Be wary of transaction apps that use QR code scanning. Don't scan any QR code to get cash. No such procedures are followed

Password management

It has to set a password to enter the password every time we enter the app. Mobile apps update automatically once installed. It can also help with security features in many cases. A transaction can be carried out in several ways. It can enter the mobile number, use the UPI ID, scan the QR code, or use the link to complete the transaction. It should double check all of this. Otherwise the money will go to someone else. Sometimes you may get caught in scams. The comparison of password management has shown in the following table 2.

Table 2: Comparison of password management

Inputs	SDMM	MFAM	CSF
100	61.01	85.27	90.33
200	59.71	84.27	89.63
300	58.41	83.27	88.93
400	57.11	82.27	88.23
500	55.81	81.27	87.53

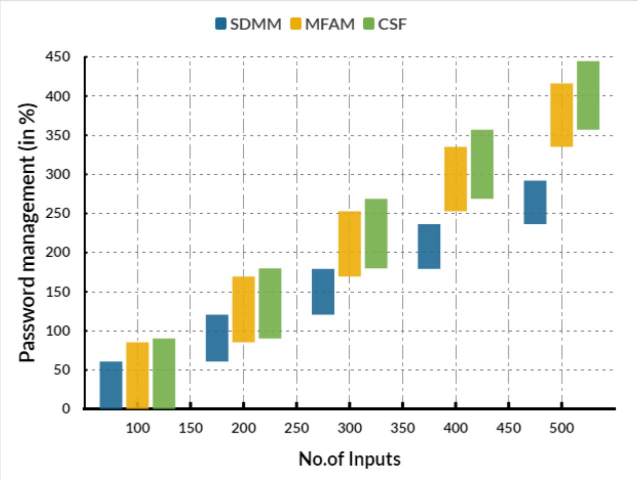

Fig.4: Comparison of password management

The fig.3 shows the password management. Try paying someone as little as Rs.5 when paying someone for the first time. Make sure the money goes to the right person. Think of mobile payments as cash payments and mobile transactions. If you lose money in any scam, it is impossible to get it back. So don't make any transaction in any hurry and doubt.

Mobile security management

A mobile phone used for transactions should be thought of as a wallet with money. Set a password for the phone. Set a secure password rather than unlocking with your face or fingerprint. Because anyone can use your line by force. But they will know only if we tell them the password. The comparison of Mobile security management has shown in the following table 3.

Table 3: Comparison of Mobile security management

Inputs	SDMM	MFAM	CSF
100	58.83	83.30	88.50
200	57.84	82.32	87.51
300	56.85	81.35	86.51

400	55.86	80.37	85.52
500	54.87	79.40	84.52

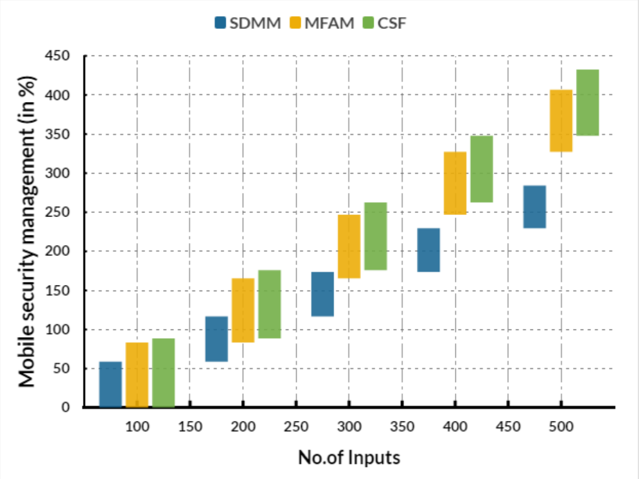

Fig.5: Comparison of Mobile security management

The fig.5 shows the comparison of Mobile security management. Turn on the feature to automatically lock you out if you enter the wrong password three times. Set a password for each transaction processor. It also need to be careful while installing any other gaming or any other app. Because malware (software designed to steal data) is injected by other fake apps.

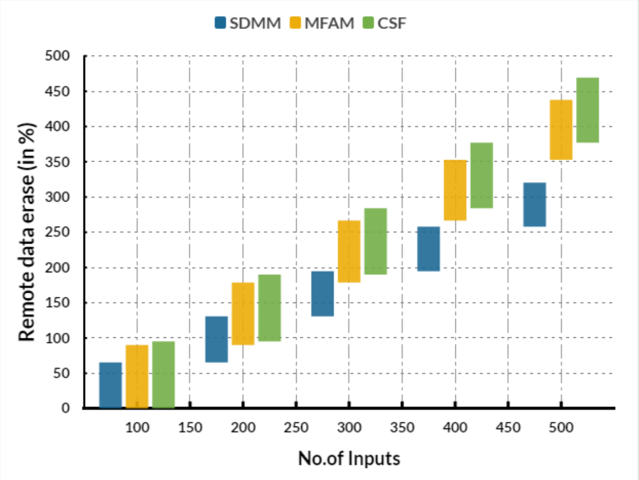

Fig.6: Comparison of remote data erases

Remote data erase

It has to set the tracking facility. Now all brand mobile phones have tracking facility. 'Remote Data Erase' so you can erase data even if you lose the phone. But the internet facility should be turned on in that phone. All in all digital transactions may be very easy but it requires a lot of caution and care. The comparison of remote data erase has shown in the following table 4.

Table 4: Comparison of remote data erase

Inputs	SDMM	MFAM	CSF
100	65.58	90.20	95.36
200	65.25	88.70	94.77
300	63.91	87.59	93.79
400	63.24	86.22	93.07
500	62.41	84.92	92.29

The fig.6 shows the comparison of remote data erase. These ransom ware malwares are capable of shutting down the main servers and network of a business and thereby completely halting the business operations of that company indefinitely. So these ransom ware malwares can cause huge financial losses and give a company a bad reputation. That's why global organizations are extremely fearful of ransom ware malware applications from cybercriminals.

4. Conclusion

As digital attacks become more sophisticated, financial institutions have had to take additional steps to protect themselves. These include implementing more secure encryption protocols, installing advanced firewalls, and conducting regular cyber security audits. Additionally, financial institutions have started investing in employee training to help staff members recognize and respond to potential cyber threats. In addition to these measures, financial institutions must also invest in cyber-security insurance. This insurance will help cover the costs associated with digital attacks, such as damages from stolen funds or data, as well as legal costs and fines. The best way to protect against digital attacks is to stay up to date with the latest cyber security trends and technologies. Financial institutions should also continue to invest in employee training and cyber-security insurance to ensure their accounts and data remain secure.

References

[1] Ramesh, G., Logeshwaran, J., & Aravindarajan, V (2022). A Secured Database Monitoring Method to Improve Data Backup and Recovery Operations in Cloud Computing. BOHR International Journal of Computer Science, 2(1), 1-7

[2] Gupta, K., & Jiwani, N. (2021). A systematic Overview of Fundamentals and Methods of Business Intelligence. International Journal of Sustainable Development in Computing Science, 3(3), 31-46.

[3] Moepi, G. L., & Mathonsi, T. E. (2021, December). Multi-Factor Authentication Method for Online Banking Services in South Africa. In 2021 International

Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-5). IEEE.

[4] Hoballah, M. M., Hammoud, Z. L., & Awada, H. M. (2019). Electronic Financial Fraud: Abstract, Definitions, Vulnerabilities, Issues and Causes. Politics of the Machine Beirut 2019 2, 9-14.

[5] Gupta, M., Rao, R., & Upadhyaya, S. (2004). Electronic Banking and Information Assurance Issues: Surveys and Synthesis. Journal of Organizational and End User Computing (JOEUC), 16(3), 1-21.

[6] Logeshwaran J, Shanmugasundaram N, Lloret J. L-RUBI: An efficient load-based resource utilization algorithm for bi-partite scatternet in wireless personal area networks. Int J Commun Syst.2023;e5439

[7] Jiwani, N., Gupta, K., & Afreen, N. (2022, March). Automated Seizure Detection using Theta Band. In 2022 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 1-4). IEEE.

[8] Gupta, M., Rao, R., & Upadhyaya, S. (2008). Electronic banking and information assurance issues: survey and synthesis. In Advances in Banking Technology and Management: Impacts of ICT and CRM (pp. 119-138). IGI Global.

[9] Adhikari, N., Logeshwaran, J., & Kiruthiga, T. The Artificially Intelligent Switching Framework for Terminal Access Provides Smart Routing in Modern Computer Networks. BOHR International Journal of Smart Computing and Information Technology, 3(1), 45-50

[10] Jiwani, N., & Gupta, K. (2019). Comparison of Various Tools and Techniques used for Project Risk Management. International Journal of Machine Learning for Sustainable Development, 1(1), 51-58.

[11] Ramesh, G., Logeshwaran, J., & Aravindarajan, V (2022). The Performance Evolution of Antivirus Security Systems in Ultra dense Cloud Server Using Intelligent Deep Learning. BOHR International Journal of Computational Intelligence and Communication Network, 1(1), 15-19

[12] Jiwani, N., & Gupta, K. (2022). Mitigating Cybersecurity Risks In Medical Devices Using Secure Implanted Techniques. Nasmin Jiwani, Ketan Gupta," MITIGATING CYBERSECURITY RISKS IN MEDICAL DEVICES USING SECURE IMPLANTED TECHNIQUES", International Journal of Creative Research Thoughts (IJCRT), ISSN, 2320-2882.

[13] J.Logeshwaran (2022, October). The Topology configuration of Protocol-Based Local Networks in High speed communication networks. In Multidisciplinary Approach in Research, Vol. 15, pp. 78-83

[14] Lloret, J., Garcia, M., Bri, D., & Sendra, S. (2009). A wireless sensor network deployment for rural and forest fire detection and verification. sensors, 9(11), 8722-8747.

[15] Das, D., Kaytal, Y., Ganesh, R., Bhattacharya, R., & Ranjan, R. K. (2021, November). AuthSHAP: authentication vulnerability detection on tabular data in black box setting. In Proceedings of the Second ACM International Conference on AI in Finance (pp. 1-8).

[16] Jasmine, J., Yuvaraj, N., & Logeshwaran, J. (2022, April). DSQLR-A distributed scheduling and QoS localized routing scheme for wireless sensor network. In Recent trends in information technology and communication for industry 4.0, Vol. 1, pp. 47–60

[17] Muhammad, K., Hamza, R., Ahmad, J., Lloret, J., Wang, H., & Baik, S. W. (2018). Secure surveillance framework for IoT systems using probabilistic image encryption. IEEE Transactions on Industrial Informatics, 14(8), 3679-3689.

[18] Gupta, M., Rao, H. R., & Upadhyaya, S. (2009). Security of alternative delivery channels in banking: Issues and countermeasures. In Socioeconomic and Legal Implications of Electronic Intrusion (pp. 305-327). IGI Global.

[19] Ramkumar, M., Logeshwaran, J., & Husna, T. (2022). CEA: Certification based encryption algorithm for enhanced data protection in social networks. In Fundamentals of Applied Mathematics and Soft Computing, Vol. 1, pp. 161–170

[20] Lin, B., Zhu, F., Zhang, J., Chen, J., Chen, X., Xiong, N. N., & Mauri, J. L. (2019). A time-driven data placement strategy for a scientific workflow combining edge computing and cloud computing. IEEE Transactions on Industrial Informatics, 15(7), 4254-4265.

[21] Logeshwaran, J. (2022, March). The control and communication management for ultra dense cloud system using fast Fourier algorithm. ICTACT Journal on Data Science and Machine Learning, 3(2), 281–284.

[22] Hong, S. (2019). Security Vulnerability and Security Measures of Kakao Bank in Industrial Environment. Journal of Industrial Convergence, 17(2), 1-7.

[23] Grabosky, P., & Smith, R. (2003). Telecommunication fraud in the digital age: The convergence of technologies. In Crime and the Internet (pp. 41-55). Routledge.

[24] Karim, Y., & Hasan, R. (2021). Taming the Digital Bandits: An Analysis of Digital Bank Heists and a

System for Detecting Fake Messages in Electronic Funds Transfer. In National Cyber Summit (NCS) Research Track 2020 (pp. 193-210). Springer International Publishing.

[25] Kovacs, L., & David, S. (2016). Fraud risk in electronic payment transactions. Journal of Money Laundering Control, 19(2), 148-157.

[26] Hasan, I., & Rizvi, S. A. M. (2022). AI-Driven Fraud Detection and Mitigation in e-Commerce Transactions. In Proceedings of Data Analytics and Management: ICDAM 2021, Volume 1 (pp. 403-414). Springer Singapore.

[27] Gupta, M., Rao, R., & Upadhyaya, S. (2005). Electronic Banking and Information Assurance Issues: Survey and Synthesis. In Advanced Topics in End User Computing, Volume 4 (pp. 233-256). Igi Global.

[28] Logeshwaran, J. (2021, December). AICSA - an artificial intelligence cyber security algorithm for cooperative P2P file sharing in social networks. ICTACT Journal on Data Science and Machine Learning, 3(1), 251–253.

[29] Edu, A. S., Agoyi, M., & Agozie, D. (2021). Digital security vulnerabilities and threats implications for financial institutions deploying digital technology platforms and application: FMEA and FTOPSIS analysis. PeerJ Computer Science, 7, e658.

[30] Logeshwaran, J., & Shanmugasundaram, R. N. (2019, December). Enhancements of Resource Management for Device to Device (D2D) Communication: A Review. In 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 51-55). IEEE.

[31] Kumar, S., Pathak, S. K., & Singh, J. (2022). A Comprehensive Study of XSS Attack and the Digital Forensic Models to Gather the Evidence. ECS Transactions, 107(1), 7153.

[32] Creado, Y., & Ramteke, V. (2020). Active cyber defence strategies and techniques for banks and financial institutions. Journal of Financial Crime, 27(3), 771-780.

[33] Sutharasan, M., & Logeshwaran, J. (2016, May). Design intelligence data gathering and incident response model for data security using honey pot system. International Journal for Research & Development in Technology, 5(5), 310–314.

[34] Rose, J. D. ., R, V. R. ., Lakshmi, D., Saranya, S. ., & Mohanaprakash, T. A. . (2023). Privacy Preserving and Time Series Analysis of Medical Dataset using Deep Feature Selection. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 51–57. https://doi.org/10.17762/ijritcc.v11i3.6201

[35] Sarangi, D. P. K. . (2022). Malicious Attacks Detection Using Trust Node Centric Weight Management Algorithm in Vehicular Platoon. Research Journal of Computer Systems and Engineering, 3(1), 56–61. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/42