[1]Mrs. Lavanya M.

[2]Dr. S. Mangayarkarasi

A Review on Detection of Cybersecurity Threats in Banking Sectors Using Ai Based Risk Assessment

JES Journal of Electrical Systems

Abstract: - The continued rise of cybercrime in the current era has frightened not only off-users but also violating financial institutions. The recent studies have shown that most financial institutions lose the credibility of their clients and their investments as a result of these attacks. The cyber-hackers involved in these types of cybercrime are now using more advanced technology. Its vigour surpasses the firewall system currently in use our network. Hence, the security needs for financial institutions are increased. So, the server management and cyber security systems getting higher end security. The cyber security aspects are is always shifting based on the attacks, but the cyber security threats are increased and create the serious discussion about the financial institutions. In General, the cyberspace describes the combination of all types of communication networks, databases, embedded processors, Internet and controllers for exchanging electronic documents. The global network environment is created by telephone wires, coaxial cables, electromagnetic waves and fiber-optic lines. Although the terms cyberspace and the Internet can be used interchangeably, it is still part of cyberspace. In simple terms, cyberspace is a connected web environment. Now, cyber-security is the process of protecting cyberspace from attack, misuse, damage and economic espionage. Cyberspace can sometimes be blocked by intrinsic vulnerabilities that cannot be eliminated. In this study, different types of cyber cards are explained in detail. And the escape processes from certain subtle attack methods are clearly stated.

Keywords: Cyber security, financial institutions, cyber crime, enhanced security algorithm, server management, cyber attacks, security optimization, Artificial Intelligence, Cyber space

1. Introduction

Now a day, the Cyber security issues are going viral on financial institutions which create the vulnerable issues. The attempts of phishing, various malware issues, different theft notifications and data breaches are continuously rising. Past few years, the world is seeing a critical medical emergency situation that can only be solved by global medical actions.

Many technology companies hire talented people to tackle various cyber crimes that are conducted dynamically. They are also trained to manage this system. Cyber-attack all depends on the general structure of the financial institution, its various hierarchical positions and the changes that are made to the financial institution's website [1]. The international relies heavily on various digital technologies. Hence, the security needs are increased to enhance the data protection. This is good news for the Info-security industry and for tech-savvy job seekers. The cyber security market is valued at N 176.5 in 2020 billion. By 2027 it is projected to be a shocking $ 403 billion with 12.5% CAGR [2].

The future of cyber security is bright. Most of the Cyber security experts are thinking a 0% job loss and huge salaries in the upcoming years. The large quantity of the cyber attacks is well planned and implemented without any opposition from security groups due to the lack of qualified workers [4]. Antivirus software of a company can identified the security threats and prevents some of the suspicious files from causing further damage. In recent days, the financial institutions have to worry about the continuum of advanced threats that allow hackers to enter the back door and remain undetected on networks for months. In recent months American businesses have become more frequent targets of hackers. Government regulations force customers to disclose the financial security breaches. However, a recent study by Veronese indicates that Americans do not know what a business will do after such an announcement. Some people know how to check their disclosure, protect their data by changing

[1] *Research Scholar, Department of Computer Science, Vels Institute of Science, Technology & Advanced studies (VISTAS),Pallavaram,Chennai, Tamilnadu.*

lakshmilavy@gmail.com

[2]*Associate Professor, Department of Computer Science,Vels Institute of Science,Technology & Advanced studies(VISTAS),Pallavaram,Chennai,Tamilnadu.*

mangai.p.s@gmail.com

passwords and cancelling credit cards and monitor their credit statements and bank statements for suspicious activity.

2. Literature Survey

N. T. Cyriac et al. [1] talk about the cyber security issues. Nowadays the advanced development of technology on the one hand has given rise to excessive growth and on the other hand has given it a parallel barrier. As the number of cyber hackers is increasing day by day, financial institutions have to constantly improve their security.

Z. S. Zainudin et al.[2] consider about the case study in Malaysian Financial Institutions. The Big businesses experiencing security breaches need to pay out some cash to improve guidance, repair financial vulnerabilities, and perform the scratch manage with the financial community. In addition to these intrinsic costs, Wall Street punishes these companies with reduced stock prices.

T. M. Mbelli et al. [3] discussed a Threat to Cyber Banking in South Africa. The financial Security communities are discussion the financial security. This suggest for SMBs to develop their data protection method. Whereas, the information faces to SMBs' system safety vulnerabilities, cautions appear to fall on hard of hearing ears.

A. K. Sood et al. [5] examine about an Empirical Study of HTTP-based Financial Botnets especially the workers working in home environment. The Remote work offers a number of benefits to companies and workers. However, the correct protocols and strategies have not been recognized with are identified to increase cyber security risks when remote employees are notified.

E. Buber et al.[6] detecting the phishing attacks from URL by using NLP techniques. at what time we imagine, of information to facilitate is at threat of being theft, we generally talk about economic information. But, the medical records are on the minds of hackers. The economic files may be cancelled along with the refunded strategies.

N. Dunstatter et al. [8] are allocating a Security Analysts to Cyber Alerts Using Markov Games. According to the financial account; the workers in the financial sector are more probable to drop quarry to phishing and communal cyber tricks than workers in other industries other than health. The fine information is that the training mechanism for them. Once workers are adequately trained, the number of failures for the fishing exam is reduced from 30% to 5%.

Uddin et al. [13] discussed about the Cyber security hazards and financial system vulnerability. In that, some proven systems need to be developed that provide the most efficient and high level of reliability that can provide the highest level of protection from cyber attacks. Furthermore, it could further strengthen the security framework if it were to be able to triple-report cybercrime in the future. Its security will be further strengthened if it is created to carry out automated security measures.

Gokhale et al [14] explained about the Dark Web Traffic Analysis of Cyber security Threats. In the Dark Web, Some Internet protocols were creating cyber problems that are detrimental to the Internet security layer. And this type of dark web monitoring is practically beyond feasible.

3. Types of Cyber attacks in financial institutions

3.1. Phishing attacks

Phishing is a type of cyber attack in financial institution. The hidden email as a weapon used for attackers. The attacker's intention was convince the financial institution’s clients, to facilitate they are getting essential information from the institution; the alert induced them to open the received messages. Once they are clicking that message, this will create a pop-up message to open some other vulnerable information. After the data collection of your network, then the hackers will install malware on sensitive computers [6]. This phishing is one of the most popular and critical hacking technique used by the hackers. The cyber security experts are monitoring the increasing use of phishing around the world. Especially, the Google found 27% more phishing websites in January 2020 than in January 2021. Most of the websites are created for the purpose of steal the financial institutions customer’s data. However, some ordinary year 2020 is the most horrible year on documentation for multiple information issues [9]. Cyber-criminals have taken benefit of the worldwide epidemic to submerge the

inbox through government relief funds and masks, hand sanitizers and antiviral followed by Govt-related phishing scams.

3.2. Ransom ware Attack

The Ransom ware restricts access to a type of malware and device or its data that infects a financial institution computer, trying to get some amount in swap for freeing them. The Ransom ware is the most dangerous and non retrievable attacks. In this virus lock your files and information and this could un-lock your data once you are getting paid some amount to them [8]. The future of cybercrime is not dark. Research by cyber security ventures shows that ransomware damage can cost businesses worldwide $ 265 billion a year and an attack rate every 10 seconds to financial institution [3]. The Ransomware threat is not anything new in current technological world, but it's a type of financial criminal activity. In the year September 2020, the famous hospital in Germany was suffered by this type of security attack.. The security attack locked all the network infrastructure of the hospital, and then creates a vulnerable environment. This means, the doctors are unable to communicate with any one and unable to access the patient reports [4]. As a result, a woman died in a life-threatening emergency situation after being taken from the city for more than an hour to hospitals due to a lack of staff at the local level. The One-third of the 5,400 businesses surveyed by Sophos.

3.3. E-Mail malware attacks

In the phase of vulnerable attacks, the email is a favourite circulation outlet for various hackers. Totally 94% of security threats are delivered via the email. Most of the cyber criminals are use this move towards in phishing scams to fix the bugs on networks. Almost shared servers are used for phishing bug in the live state in US. Some of the information that usually comes in your inbox may even be a cyber attack emails. That means a link containing a few short messages will be sent via email [6]. That information will send your information to the hacker as soon as you click on it.

3.4. Mobile malware attacks

The Photos and videos can be captured by the mobile you normally use. This mobile application is a tactic that most hackers use to take your information lightly. Once a mobile application with specific vulnerability information is installed on your mobile phone, it starts stealing information [7]. As a result, it not only steals information but also steals some photos and video. Doing so makes the job of cyber thieves much easier to change. For example they can easily take and use the most important things like OTP coming to you from your financial institution. You can easily withdraw money from your account or do transfer work [8].

4. Cyber attack detection and Security

The impact of cyber attacks, which can be very challenging and serious, can have a huge impact on financial institutions. And given its versatility, its malignant effects may be undetectable in the short term [15]. On average, it takes about 280 days to detect and stop a cyber attack. It takes about 197 days to identify a typical system threat, but some violations can avoid detection for a long time. How long it takes for your company to eliminate the threat depends on how strong your security system is. Once diagnosed, the attack often lasts another 69 days on average. Companies that can control attacks in less time can save hundreds of thousands of dollars on recovery costs [18].

Today, the best security techniques available are encryption, virus, firewall, digital signatures and two-factor authentication. Companies are responsible for protecting customer data and protecting it from unauthorized access [19]. While these cyber security statistics are restless, part of a company's obligation is that its cyber security system has everything it needs to succeed [20].

4.1. Make sure all the information's are updated:

Check and verify all your website details are updated. Each part of software recognized to humans is revealed from side to side bugs and potential security threats. These holes will remain even if kept upgraded. Everything it takes is vulnerability and can be accessed by cybercriminals. By making sure you make regular updates, the use of security holes is minimized. This is especially important for those who use open source web tools. In general, many of the open source software tools are affected it selves. Against this, there are many ways you can get tested.

4.2. More secure via Strong Passwords

The simpler the passwords you use in general, the more likely it is that cybercrime will occur. As a result, unwanted hacking activities occur in the applications of your financial institution. Thus not only the financial institution but also its customers are severely affected. This causes huge monetary damage. So the passwords in the important software used in most financial institutions should be very neat and easily predictable by anyone. This enhances the reputation of the company and enhances security measures to prevent cybercriminals from smoking inside.

4.3. Secured network via SSL certificate

Most of the network utilizes in financial institutions are know much about HTTP and SSL. Now a day, most of the financial institutions are authorized only SSL encryption certificate to ensure the network protection. SSL certifications are not mandatory for application websites and web portals but it is very mandatory for the payment transitions performed by the financial institutions. Most of the web hosting providers is sell the SSL certification and HTTPS (Secured Hypertext Transfer protocol). Initially a chipper text is added in your hosting sites. Then this provides a security verification check for the website contents and other sub domains. After completing the security parameter checking, then that creates a report. Based on the report the certification parameters are evaluated. These evolution reports redirect you to the SSL certification registration. Once you complete all the security check then the SSL certification successfully installed in your server. This reflects for your main domain and all you hosted files including the sub domain and mail server files.

4.4. Backup and restore

Generally most of the network users are not aware of this information back-up system. Suddenly your server was suffered by the ransomware or phishing attack there is no chance to restore them immediately. In that scenario the back-up and restore option was help you to restart works without any extra spending payment for hackers. Initially all the files and email information are stored in the database of your network. The source and database are consecutively updated based on the information performed every day. Then the restore points are created as per the system storage. This will create a point for system and network functionalities. This method is one of the easiest ways to restore the network information.

4.5. Keep your customer information secure

The nature of the networks you use in general creates the risk of somehow leaking your information. The reason for that are you. However, none of your information will be published on the network without you entering it. This is what we discussed earlier about SSL, which is the secure placement of information from one point to another during SSL, or secure socket layer transfer. Unfortunately, only SSL keeps the transfer secure. Be sure to ensure the security of your website as soon as it is reached! If possible, do not store sensitive data if you do not need it. The encryption name comes up here because it is practically impossible. It comes with password encryption and other bits of information for user accounts on some sites like WordPress. If you want to host your dedicated website on your own server, then you ensure all the security parameters are performed well. The web coding failure invites the hackers to hack all your information. So ensure the data privacy and security getting higher attention.

4.6. Secure your data transfer via VPN

The virtual private network application is currently being widely used. When you access the Internet through proxy servers it is very difficult to steal your information or hack your account. This means that hacking hackers can cause your IP address to be compromised. And by the time your IP address is detected and hacked, your work will be done. So it is considered a little better way.

5. Inference and Discussions

The Financial institutions should be compelled to pay more attention to relevant cyber security practices. There are also methods that positively motivate current data to further ensure its security [16]. In today's world technology has made a huge difference in the way people live their lives. There is a situation where it is difficult to live without these. The situation has developed where our descendants have to get used to playing traditional

games on the computer [21]. We need to know about the cyber crimes that are talked about so much today in these technologies. Cybercrime is a crime committed by targeting or using information technology in financial institutions [24]. More specifically, it is the act of stealing or erasing information and financial institution thefts using or hacking into the Internet, mobile and many other devices.

One of the common causes of cybercrime in financial institutions is the inability to effectively protect the financial institution's servers and information. It is through these loopholes that various cyber crimes continue to take place. And the impact of these cyber crimes is causing a lot of problems for the customers of that financial institution. Keeping data from financial institutions secure can reduce problems by up to 90 percent. That is, information about the customer often goes unnoticed by cybercriminals while preventing information theft. Thus they cannot commit any cyber crimes. Instead, if financial institution customer information is available, hackers can easily access them and get everything they need from them. As a result money will be stolen from their account. Due to this most financial institutions can criticize the irresponsibility of the customer. But they do not know that the crimes that happen on their server are the ones that cause the customer problems. And a customer is less likely to be familiar with those financial institution technologies. Thus he has no idea what is going on there. But in the end it is the customer who suffers.

Here some of the crimes are listed, that are considered to be the most important of the various cyber crimes in financial institutions are mentioned above

- Data Hijack in Financial institutions is an early technology that steals information. Ransomware is an improved example of this method. It is a modern cyber crime to keep your data hostage and use it to extort money from the financial institutions. You will be bargaining for the information that will be held hostage. Your data will be refunded upon receipt of the final amount of the bill. As a result, financial institutions are more likely to incur large sums of money. So financial institutions need to fix this problem first
- The Deleting or modify the various customer details are the type of problems. There the premium customer details or other personal information was modified by the cyber criminals. Then the user was unable to utilize the financial activities. Then the financial institution was suffered and lost the customer.
- The Cheating on strangers on the Internet Stealing information from computer and information technology devices (Cyber Hacking, Malware and Virus attacks, DOS attack etc) in financial institutions
- The Misuse of other people's information or account details in financial institutions is the vulnerable activity carried by the cyber attacker. They theft the customer details including the log-in credentials. Then the purchase and other financial activities are performed by the attacker with the use of this particular customer attack.
- The Cyber security threats by email (like phishing and email vulnerabilities) and internet call in financial institutions
- Cyber Violation crimes, IPR violations, Credit card frauds, EFT frauds in financial institutions

The main responsibility of those financial institutions is to protect a customer from any of the above problems. When it comes to research, accounts are opened on the website created by the financial institution and the financial institution faces its technical work. Minor security vulnerabilities can also come from customers. But most of it happens on the servers of financial institutions. Therefore proper procedures must be followed to effectively monitor and manage those servers. Doing so can prevent most cyber crimes.

More and more crimes are being committed on the financial institution's website to deceive customers. For example, cybercriminals are at risk of stealing their information when customers enter their information on fake websites, such as financial institution website. Customers are also required to enter other secure information that changes their password only after verifying the security of the website they use twice a day. Failure to do so will result in the financial institutions not taking responsibility for your problems

6. Future Work

Some modern structures need to be developed to incorporate more security features related to financial institutions based cyber security and cyber risk management [17]. The cybercrime cannot be reduced if you or your financial institution's software is well designed. The cybercrime can be prevented only if each of their variants is properly

documented. Thus an improved algorithm will plan to design for financial institutions. An elevated time stamp design with a code certification system designed to perform these actions is to be developed. This encryption certificate will be digitally signed [25]. This will make it easier to identify who issued this signature in financial institution. It also saves information about signature design changes made to your financial institution software. This not only provides adequate security for your financial institution and your software but also helps you to manage it effectively. This will ensure that no harm is done to your software.

To improve the design of the financial system software, its personal use and security for its drivers, digital certificates are used here to sign the code. The software developer uses a private key to attach a strong digital signature to the code signature certificate issued by the Certification Authority. The public key is used to decode the signature generated by the developer during the time stamp creation process. It decodes the user's signature using special software or the software's personal application key. The software immediately searches for the required root certificate to add the used signature to the verified ID. The software system uses another hash code to sign the hash code used when downloading its application. Next, if the root and hash here are correct, the connection services will start immediately. If the root and hash do not match correctly, the services will not run. Instead it will interrupt the work and display a warning message.

7. Conclusion

The Financial institutions and their clients are making various efforts to prevent most cyber crimes. The result is a massive reduction in crime. The solidarity of financial institutions and customers has made cybercriminals think a bit. But their improved tactics continue to threaten financial institutions again. Financial institutions are thus forced to continue to improve their security operations. Further ongoing updates may also give customers some inconvenience. So, the financial institutions need to keep up-to-date with information about their safety for customers who do not know or understand technology. In this way cyber criminals can be completely prevented from coming from outside. But it is very difficult to find them where they are inside the financial institution. That means finding cybercriminals who are the job or client of a financial institution can be very challenging. Thus, no matter how much security is put in place, cyber thieves will find ways to break it easily. Thus, the identification of the cyber criminals is more difficult

Reference

[1] N. T. Cyriac and L. Sadath, "Is Cyber Security Enough- A study on Big Data Security Breaches in Financial Institutions," 2019 4th International Conference on Information Systems and Computer Networks (ISCON), 2019, pp. 380-385, doi: 10.1109/ISCON47742.2019.9036294.

[2] Z. S. Zainudin and N. Nuha Abdul Molok, "Advanced Persistent Threats Awareness and Readiness: A Case Study in Malaysian Financial Institutions," 2018 Cyber Resilience Conference (CRC), 2018, pp. 1-3, doi: 10.1109/CR.2018.8626835.

[3] T. M. Mbelli and B. Dwolatzky, "Cyber Security, a Threat to Cyber Banking in South Africa: An Approach to Network and Application Security," 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), 2016, pp. 1-6, doi: 10.1109/CSCloud.2016.18.

[4] Y. Xiang, "Defending against Large-Scale and Coordinated Attacks in the Ubiquitous Environments," 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, 2011, pp. 7-8, doi: 10.1109/TrustCom.2011.4.

[5] A. K. Sood, S. Zeadally and R. J. Enbody, "An Empirical Study of HTTP-based Financial Botnets," in IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 2, pp. 236-251, 1 March-April 2016, doi: 10.1109/TDSC.2014.2382590.

[6] E. Buber, B. Dırı and O. K. Sahingoz, "Detecting phishing attacks from URL by using NLP techniques," 2017 International Conference on Computer Science and Engineering (UBMK), 2017, pp. 337-342, doi: 10.1109/UBMK.2017.8093406.

[7] L. Mutegi, D. Gichuki and J. Sevilla, "IT security service commoditization: The case of financial institutions in Kenya," 2016 IST-Africa Week Conference, 2016, pp. 1-9, doi: 10.1109/ISTAFRICA.2016.7530642.

[8] N. Dunstatter, M. Guirguis and A. Tahsini, "Allocating Security Analysts to Cyber Alerts Using Markov Games," 2018 National Cyber Summit (NCS), 2018, pp. 16-23, doi: 10.1109/NCS.2018.00008.

[9] B. Vedral, "The Vulnerability of the Financial System to a Systemic Cyberattack," 2021 13th International Conference on Cyber Conflict (CyCon), 2021, pp. 95-110, doi: 10.23919/CyCon51939.2021.9468291.

[10] A. K. Kassem, A. E. Salam AL HAJJAR, B. Daya and P. Chauvet, "A Proposed Methodology for Cyber Security Mechanism According to the Most Popular Detected Attacks for University Web Application," 2018 Second World

Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 2018, pp. 215-219, doi: 10.1109/WorldS4.2018.8611626.
[11] M. M. Rana and N. Dahotre, "IoT-Based Cyber-Physical Additive Manufacturing Systems: A Secure Communication Architecture, Research Challenges and Directions," 2021 6th International Conference on Inventive Computation Technologies (ICICT), 2021, pp. 216-219, doi: 10.1109/ICICT50816.2021.9358643.
[12] P. C. Mondal, R. Deb and M. N. Huda, "Know your customer (KYC) based authentication method for financial services through the internet," 2016 19th International Conference on Computer and Information Technology (ICCIT), 2016, pp. 535-540, doi: 10.1109/ICCITECHN.2016.7860255.
[13] Uddin, M.H., Ali, M.H. & Hassan, M.K. Cybersecurity hazards and financial system vulnerability: a synthesis of literature. Risk Manag 22, 239–309 (2020). https://doi.org/10.1057/s41283-020-00063-2
[14] Gokhale, C., Olugbara, O.O. Dark Web Traffic Analysis of Cybersecurity Threats Through South African Internet Protocol Address Space. SN COMPUT. SCI. 1, 273 (2020). https://doi.org/10.1007/s42979-020-00292-y
[15] Dalal, R.S., Howard, D.J., Bennett, R.J. et al. Organizational science and cybersecurity: abundant opportunities for research at the interface. J Bus Psychol 37, 1–29 (2022). https://doi.org/10.1007/s10869-021-09732-9
[16] Sarker, I.H., Kayes, A.S.M., Badsha, S. et al. Cybersecurity data science: an overview from machine learning perspective. J Big Data 7, 41 (2020). https://doi.org/10.1186/s40537-020-00318-5
[17] Cremer, F., Sheehan, B., Fortmann, M. et al. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract (2022). https://doi.org/10.1057/s41288-022-00266-6
[18] Wylde, V., Rawindaran, N., Lawrence, J. et al. Cybersecurity, Data Privacy and Blockchain: A Review. SN COMPUT. SCI. 3, 127 (2022). https://doi.org/10.1007/s42979-022-01020-4
[19] Klenka, M. Aviation cyber security: legal aspects of cyber threats. J Transp Secur 14, 177–195 (2021). https://doi.org/10.1007/s12198-021-00232-8
[20] Domingo-Ferrer, J., Blanco-Justicia, A. Ethical Value-Centric Cybersecurity: A Methodology Based on a Value Graph. Sci Eng Ethics 26, 1267–1285 (2020). https://doi.org/10.1007/s11948-019-00138-8
[21] Kandasamy, K., Srinivas, S., Achuthan, K. et al. IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP J. on Info. Security 2020, 8 (2020). https://doi.org/10.1186/s13635-020-00111-0
[22] Waqas, M., Tu, S., Halim, Z. et al. The role of artificial intelligence and machine learning in wireless networks security: principle, practice and challenges. Artif Intell Rev (2022). https://doi.org/10.1007/s10462-022-10143-2
[23] Haque, M.F., Krishnan, R. Toward Automated Cyber Defense with Secure Sharing of Structured Cyber Threat Intelligence. Inf Syst Front 23, 883–896 (2021). https://doi.org/10.1007/s10796-020-10103-7
[24] Kure, H.I., Islam, S. & Mouratidis, H. An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Comput & Applic (2022). https://doi.org/10.1007/s00521-022-06959-2
[25] King, T.C., Aggarwal, N., Taddeo, M. et al. Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. Sci Eng Ethics 26, 89–120 (2020). https://doi.org/10.1007/s11948-018-00081-0