International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 10 | Oct 2021 www.irjet.net p-ISSN: 2395-0072

Survey on Development of an Sustainable Cyber Security Model on Identification and Prevention of Non-Detectable Key-Logger Trojan Horse, RFID Theft and Sim Cloning Attacks.

Prof. Vina M. Lomte[1], Shubham S. Patil[2], Anuja Lokhande[3], Kartik Mogal[4], Komal Mohite[5]

[1-5]*Department of Computer Engineering, RMD Sinhgad School of Engineering, SPPU, India.*

Abstract - *A cyber-attack is malicious attempt by a person or organization to gain unauthorized access, steal data or cause damage to computers and destroying sensitive information. So in this study we will quickly detect and effectively respond to mitigate sophisticated key-logger Trojan horse and minimize the impact on sensitive data theft. Similarly securing and stating prevention majors in RFID and bundle a proper security protocol package in order to protect Sim cards from Sim cloning cyber-attacks. Key-logger is software which is installed on your system and will fetch everything you type and attacker will easily get your information. Radio-Frequency Identification Technology (RFID) in this technology RFID theft occurs when someone uses their own RFID reader to trigger the RFID based financial access cards. and Sim cloning is the attack in which a SIM card is duplicated and after cloning the cloned SIM card's information is transferred onto the another SIM card and attacker can extract the SIM card's Authentication key(ki) and IMSI(Information Mobile Subscriber Identifier). Because of this digital industry faces billions of dollars financial loss, data loss and system or server crashes. There are so many organizations had experienced a data breach caused by issues like devices or documents being lost or computers being left unattended. So our purpose of this survey based on cyber-attacks is to develop an sustainable cyber security model in future as well as an proper system architecture to help prevent these types of cyber-attacks.*

1. INTRODUCTION

From the past few years, technology has grown immensely and due to its ease of understanding, it is being used by people of all age groups. As the use of technology is increasing vigorously, the severity of cyber-attacks has also increased tremendously. Due to poor knowledge of cyber-attacks and neglecting the importance of cyber security many organizations and individuals have witnessed financial loss as well as data loss. However, the year 2020 has shown a whole new level of cyber-attacks. As the covid-19 pandemic introduced a new way of work to the world, it has accelerated cyber-attacks as well as data breaches. Many renowned companies were targeted and were hacked for essential data worth billions of rupees. Recently, In 2021,700 million LinkedIn users' data were exposed including email addresses, phone numbers, workplace information, account ids, links to their social media accounts, and gender details. In 2020 over 600 million accounts data of Sina Weibo website were leaked. Similarly, a 17-year-old hacker and his group breached twitter's network and grabbed control of Twitter accounts of high-profile users, and stole over $118,000 worth of bitcoin. Laundry's 63 restaurants' payment card details were hacked by malware targeting the restaurant's order entry systems which have card readers attached.

In this study, the Author has mainly researched three attacks that cause breaching of sensitive and valuable data. It includes key-logging malware, RFID theft in banking transactions, and Sim cloning attacks.

Key logger or keystroke logger is a program that monitors and logs all the keystrokes entered by the user through the keyboard including passwords, user names, and banking details. It can be programmed to monitor any type of data such as keystrokes, screens, and retrieving files from the user's system. Key logger logs all keystrokes and stores this log file into the local device and then sends it to a server from where the hacker can access this sensitive data. Key logger Trojan can be installed to the victim's system without any permission along with the regular files and commonly used applications; this can be achieved by practicing social engineering. As key logger Trojan can enter into the system in the form of regular executable files, it can simply pass through antivirus software without detecting them. The authors studied several research papers and this study has shown that key

logger Trojans are advancing into new versions making it difficult to detect by standard antivirus scanners and windows defender.

RFID or Radio-Frequency Identification Technology is a wireless technology which works on Radio Waves and it is used in many industries for access control, supply chain logistics. In RFID there is one microchip and antenna. A microchip contains identifying information and an antenna that transmits the information or data to the reader. Reader can read the information which is stored in tags. Any organization or industry could be at risk of cyber-attack and there are many organizations due to cyber-attack affected and duped in financial loss, data loss. In the year 2013, information of 70 million credit cards of an organization called "Target" was stolen by using Card Skimming Malware attack.

The subscriber identity module (SIM) card is the transmitter of the signal to the mobile and tower. Our SIM cards contain two secret codes or keys called IMSI (international mobile subscriber identity) and KI (Authentication Key). These codes are the identifier of the Sim card .when someone gets IMSI and KI codes of Sim card then the attacker programs it into programmable empty SIM card for hacking and this procedure is known as Sim cloning. In the SIM cloning attackers create duplicate copy of the real SIM card. Not every SIM card is clone able, only some SIM card are clone able .now currently COMP128v1 architecture based SIM cards are mostly cloned. COMP12v1 is a first version of COMP12v architecture SIM cards. Because of SIM cloning attack we lost our important data like details of account information, financial information or other important document .so we will ensure to state the process between the subscriber and network which inhibits attacker to decrypt the encrypted and the operator in Sim cloning cyber-attacks and prevention majors against it.

2. Literature Survey

Table -1: Deep Literature Survey of Current Technologies

Sr. No.	Paper Title Publication Details	Pre-Processing	Feature Extraction and Classification	Accuracy	Post Processing	Research Gap Identified
1.	Keyloggers:silent cyber security weapons Dr Akashdeep Bhardwaj, Dr Sam Gondar, ELSEVIER, Volume 2020, Issue 2, February 2020, Pages 14-19,10.1016/S1353-4858(20)30021-0	key loggers are almost impossible to detect and remove because privilege level at which it executes is higher than typical malware.	virtual keyboards with randomly exchanging vertically adjacent keys	78%	The proposed layout for virtual keyboards involves randomly exchanging vertically adjacent keys from the existing QWERTY layout, using random spacing. This can provide high accessibility and high security simultaneously	Not included the Anti-Key-logger system which successfully determines developed malware in targeted system.
2.	New safety measure to protect the 3G/4G SIM cards against cloning Nabil Zidouni1, Salim Chitroub1, Hakima Chebout1 and Nesrine Boukais1 1LISIC Laboratory,	mobile phones become the preferred targets of attacks and consequently the mobile security as well as the mobile phone security are now increasingly	RESi subdivided into 4 sub-messages of 16 bits, IKi subdivided into 8 sub-messages of 16 bits and CKi subdivided into	72%	new security mechanism that could be implemented in the mobile phones for a more safety measure in cellular network is proposed. It permits of reinforcing at the	Algorithm cracked for Sim cloning attack is the 1st version of COMP128 in the future people will try to compromise these versions as well. More advanced operators have

	Telecommunication Dept., Electronics and Computer Science Faculty, USTHB BP. 32, El-Alia, Bab-Ezzouar, 16111, Algiers, ALGERIA	important in mobile computing	8 sub-messages of 16 bits.		same time the authentication of the subscriber and data encryption communicated between subscriber and network.	switched to the COMP128v2 and COMP128v3 algorithms which increase the number of RAND-SRES packets so that the Ki key can not be easily deduced.
3.	Virtual Machine Introspection for Anomaly-Based Keylogger Detection Huseyn Huseynov,Kenichi Kourai,Tarek Saadawi,Obinna Igbe,IEEE,2020,10.1109/HPSR48589.2020.9098980	to provide secure environment by constantly checking VMs for the presence of keyloggers using AIS based technology	virtualization tool (KVMonitor), genetic algorithm based application, artificial immune system (AIS) based algorithm	82%	VMI and AIS based approach for detecting malicious activities on Linux based VMs provides efficient way of monitoring VMs	1) hidden keyboard simulator can be developed 2)existing detection system can be expand by adding up Linux Kernel-based keyloggers.3)the proposed system can be try to run on cloud based VPN server
4.	KeyGuard: Using Selective Encryption to Mitigate Keylogging in Third-Party IME Jia Wang, Brent Lagesse ,2020,arXiv:2011.10012	intercepting the keystroke events triggered by a user and encrypting them before sending them to the third-party IME	Keyguard,Xposed framework,Google sample IME	87%	Keyguard enables third party IME to store encrypted information and send it on remote server	1)to use Key Guard we need to intercept keystroke event that require user's device to be rooted mainly to install Xposed framework. 2)Xposed framework needs to know exactly which class and which method to hook.
5.	A Novel Approach of Unprivileged Keylogger Detection Ahsan Wajahat; Azhar Imran; Jahanzaib Latif; Ahsan Nazir; Anas Bilal,IEEE,25 March 2019,10.1109/ICOMET.2019.8673404	to forbid userspace keylogger from stealing confidential data by matching I/O of all processes with some simulated activity .	Open source keylogger-s key email version 7.0, Spybot version 1.2 and Morsa-keylogger version 1.8. ,2) keylogger used.	72%	keylogger response is displayed by matching the input from keystrokes and with the output i.e.I/O designs that are delivered.	
6.	The Process of Reverse Engineering GPU Malware and Provide Protection to GPUS Yazeed Albabtain; Baijian Yang, IEEE,06 September 2018, 10.1109/TrustCom/BigDataSE.2018.00248	to remove malware, namely the Win Jelly and the Demon keylogger, that escapes detection by Graphics Processing Units (GPUs) as a hideout.	OpenCL	74%	zero-out memory technique presented in this paper will help GPU developers to remove the malware completely from the system	developing a tool using the OpenCL or CUDA frameworks
7.	Social Engineering Solutions for Document Generation Using Key-Logger Security Mechanism and QR Code Nikhil Tekawade; Shruti Kshirsagar; Shripad Sukate; Leena Raut; Shubhangi Vairagar,IEEE, 25 April	The proposed system can generate and retrieve certificates and documents through e-documents.	QR code, key-logging Encryption and Decryption using AES algorithm,One Time Password(OTP) system	78%	Proposed conventions improve user experience and resists challenging attacks such as keylogger and malware.	The database needs to be upgraded according to the storage and also the part of user interface.the servers for the system smooth running be made distributed. the auto

	2019,10.1109/ICCUBEA.2018.8697420					filling of the previous filled data of particular users..
8.	Keystroke logs: Are strong passwords enough? Darshanie Sukhram; Thaier Hayajneh, IEEE,08 January 2018,10.1109/UEMCON.2017.8249051	Three keylogging software are tested against two anti-keylogging programs to identify what information is captured and which method of protection is stronger	Phrozen Keylogger Lite,Actual Keylogger , Refog Free Keylogger,SpyShelter Firewall,MalwareBytes Anti-Malware	76%	In addition to using password managers and two factor authentications, organizations and enterprises need to install validated anti-keylogging software	
9.	Keylogger Is A Hacking Technique That Allows Threatening Information On Mobile Banking User Adam Prayogo Kuncoro; Bagus Adhi Kusuma, IEEE,2019,10.1109/ICITISEE.2018.8721028	the possibility of attacks are discussed that can threaten users of mobile banking services using keylogger	static forensic process is used to perform a detailed analysis phase	86%	Keylogger application is used in order to get all stored information results from typing on virtual keyboard in smartphones	tests related to iOS and Windows Phone can be conduct with similar case simulations.
10.	Infringement of Prevention Technique against Keyloggers using Sift Attack Arun Pratap Singh; Vaishali Singh,19 December 2019,IEEE,10.1109/ICACAT.2018.8933805	Sift attack allows extraction of information on the basis of algorithm. Paper proposes a concept that can break security approach made against keylogger that may conceal passwords.	When actual keystrokes are visible pattern can be analyzed. Every keystroke can be recorded and actual key can be observed.	82%	The system is able to crack the security concerns of previously implemented system which claims to prevent the confidential data against keylogger or any spyware programs by encryption	system can be developed which can capably encrypt the login credentials by encrypting the letters among random string of alphanumeric keys at every session instead of repeated patterns
11.	Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines Danial Javaheri; Mehdi Hosseinzadeh; Amir Masoud Rahmani,IEEE Access (Volume: 6),07 December 2018,IEEE,10.1109/ACCESS.2018.2884964	paper provides a novel method for detection, tracking and confronting the stealth and obfuscated spyware and ransomware including keyloggers, screen recorders, and blockers	Linear Regression, JRIP and J48 decision tree algorithms(to recognize malwares),	92%	novel and efficient method has been proposed based on the dynamic behaviour analysis to recognize the process and executable files of the spyware	
12.	C. Occhiuzzi(1,2), S. Amendola(1,2), S. Nappi(1,2), N. D'Uva(2) and G. Marrocco(1,2) IEEE 2019 https://doi.org/10.1109/RFID-TA.2019.8892049	Introduces the possible architectures and the relative implementations in real scenario.	RFID technology in Industry 4.0 scenarios	88%	RFID passive technology can be considered a valid and applicable instrument.	solve issues related to high temperature and high speed operation conditions must be seriously
13.	Review and Analyzing RFId Technology Tags and Applications 1Ag. Asri Ag. Ibrahim, 1,2Kashif Nisar, 1Yeoh Keng Hzou, 2Ian Welch, IEEE 2019, https://doi.org/10.1109/AICT47866.2019.8981779	This review paper is based on (RFID) technology, Wireless Sensor Networks	Different types of smart home technologies are catalogued	74%	RFID that it able to provide privacy and differentiate the target user	further study on wide-ranging applications RFID technology.

14.	Fast Identification of Blocked RFID Tags Xiulong Liu Xin Xie Xibin Zhao Keqiu Li Alex X. Liu Song Guo Jie Wu, (Volume: 17, Issue: 9, Sept. 1 2018), https://doi.org/10.1109/TMC.2018.2793219	studies how to quickly and completely identify the valid RFID tags that are blocked	Protocol are used Aloha Filtering (AF) and Poll Listen (PL)	84%	The simulation results reveal that AF+PL+SEBU can identify the blocked tags with an accuracy of 100%.	
15.	EXPLOITING RFID FOR BUSINESS TRANSFORMATION: A STRATEGIC ANALYSIS VIS-À-VIS AGRICULTURAL BANK OF Dr. Harman Preet Singh Department of Management & Information Systems, College of Business Administration, University of Hail. CHINA, Jan 2019	The applications of RFID in various business situations have been studied	Maxi-Maxi Strategy (SO Strategy),Mini-Maxi Strategy (WO Strategy):	79%	These applications include management of inventory stock outs, preventing theft of items, traffic management.	Minimize connectivity problems and improve RFID infrastructure.
16.	Indoor Localization Systems for Passive UHF RFID Tag Based on RSSI Radio Map Database, Progress In Electromagnetics Research M Mugahid Omer1, Yachao Ran2, and Gui Yun Tian1, 2, Vol. 77, 51–60, 2019	RFID system to estimate the indoor position of a passive tag utilizing a received signal strength indicator (RSSI).	Passive tag utilizing a received signal strength indicator (RSSI).	83%	It is clear that the accuracy is influenced by a number of coefficients in an indoor environment.	Find different types of signals such as phase and RSSI can be combined to improve localization accuracy
17.	RFID-Based Library Management System with Android Mobile Access Application Roben A. Juanatas, Irish C. Juanatas, December 11–12, 2019, Amity University Dubai, UAE, 978-1-7281-3778-0/19/$31.00 ©2019 IEEE	Presents the used of RFID in library management system and Android mobile application	Attributes-functionality,usability,relibility,performance,security	85%	RFID speeds up library routine procedures and allows library staff to perform more user-service activities.	we have to apply AJAX concept so that it can be instantly checking user's input and provide immediate feedback
18.	Performance analysis of binary search based RFID anti-collision algorithms Meryle Mvoulabolo1, Tebello N.D. Mathaba2, Marcel O. Odhiambo3, May 08,2020	Performance comparison of different binary search based anti-collision algorithms is done	improvements the basic search algorithm and its working principle.	77%	Performance comparison of different binary search based anti-collision algorithms is done	we will define OBS and ANA algorithms are more suitable for high density application
19.	Multiple Resolution Bit Tracking Protocol for Continuous RFID Tag Identification, Weiping Zhu∗, Mingzhe Li∗, Jiannong Cao†, Zongjian He‡ and Rong Xie∗§, 2019 IEEE	Propose a new approach called multiple resolution bit tracking protocol (MRB) to improve performance	Protocol to identify the tags in the interrogation region of an RFID reader as quickly as possible.	81%	According to our evaluation, MRB can achieve 3.7 tags per unit time when identifying tags.	
20.	, Active RFID Tag with Better Tracking Range for Automotive Applications Arvind Lakshmanan , Vivek Maik SRM Institute of Science and	Describes a system that will collect the data which will be produced by the RFID reader.	implemented a system that will use an active RFID tag .	72%	This process will find the objects in a few minutes, and save time.	If it is done manually it will take hours to find or in some cases days.

	TechnologyIEEE 2019					
21.	Design of Robust Detection System for Printable Chipless RFID Tag Alphabet Letters Oussama Boularess, Taoufik Aguili , Jawad Yousaf Department of Electrical and Computer Engineering , , 978-1-7281-4064-2019 IEEE	Presents a novel chipless rad (RFID) tag design method for Latin alphabet	s alphabet letters (a, b and c) are realized using copper etching on thin dielectric substrate (TLX-8) backed by a ground plane.	78%	EM signature of a novel chipless RFIDletter tag using three alphabetic letters (a, b, and c) was investigated experimentally	Define more chipless alphabet tag IDs have simple reconfigurable design.

3. Algorithmic Survey

Table -2: Algorithmic Survey of Research Studies

Sr. No.	Paper Title	Algorithm Used	Time Complexity	Space Complexity	Accuracy	Advantages / Disadvantages
1.	Key loggers: silent cyber security weapons	Backdoor algorithm	O(2KN)	-	76%	-
2.	New safety measure to protect the 3G/4G SIM cards against cloning	COMP128v1	O(K)	-	82%	There are 3 algorithms out of which this one is only cracked by hackers which is the major disadvantage of this algorithm.
3.	Fast Identification of Blocked RFID Tags	binary-search algorithm	O(log n)	O(1)	86%	It does not scan each element in the list and It takes less time to search an element
4.	Review and Analysing RFID Technology Tags and Applications	Process Data Algorithm and K-Means' algorithm	O (LKN)	O (N(D+K))	80%	Easily adapts to new examples. Generalizes to clusters of different shapes and sizes, such as elliptical clusters.
5.	Exploiting RFID for Business Transformation: A Strategic Analysis vis-à-vis Agricultural Bank of China	Decision Tree Algorithm	O(m · n)	O(depth)	72%	their outputs are easy to read and interpret without requiring statistical knowledge
6.	Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines	Support Vector Machine (SVM) algorithm	O(N^3)	O(N^2)	76%	SVM works relatively well when there is a clear margin of separation between classes
7.	Social engineering solutions for document generation using key-logger security mechanism and QR code	AES algorithm	O(k)		82%	AES can be implemented on both hardware and software
8.	Active RFID Tag with Better Tracking Range for Automotive Applications	The least squares fit approach	O(n 2 log n)	O(n)	70%	Merits of least square method is completely free from personal bias of the analyst
9.	Indoor Localization Systems for Passive UHF RFID Tag Based on RSSI Radio Map Database	K-NN algorithm	O(n*m)		86%	Quick calculation time
10.	Social engineering solutions for document generation using key-	AES algorithm	O(k)		82%	AES can be implemented on both hardware and software

	logger security mechanism and QR code					
11.	Virtual Machine Introspection for Anomaly-Based Keylogger Detection	Negative selection algorithm (NSA)	O((l – r) · 2r · NR)	O(1)	-	-
12.	A Novel Approach of Unprivileged Keylogger Detection	Dendritic Cell Algorithm	O(n(2))	-	-	-

4. Live Survey

Table -3: Live Survey of Recent Cyber Attacks on various Organizations

Sr. No.	Attack Title	Attack Type	Organization	Attacker Details	Year	Loss- Financial / Data
1.	God User	Data Scraping & Logging	LinkedIn	Anonymous	2021	**700 M accounts information leaked**
2.	Laundry's Data Breach	Malware containing Keylogger	Laundry's Restaurants	Anonymous	2020, 2015	**$ 20 M Fine by US Federal Government**
3.	Sina Weibo Attack	Database Keylogging	Sina Weibo	Anonymous	2020	**600 M accounts information leaked**
4.	Hawk Eye Malware	Malware containing Keylogger	IBM	Anonymous	2019	**Unknown**
5.	Cathay Malware key logger	Trojan containing key logger	Cathay Pacific Airlines	Anonymous	2018	**9 billion users data breach**
6.	Marriott International	Key logging of guest reservation database	Marriott International	Chinese Group	2018	**18.4 M Euros Fine by UK Govt.**
7.	Equifax Credit Bureau	Vulnerability in Apache Struts open source	Equifax	Anonymous	2017	**143 M accounts information of US Citizens**
8.	Uber	Uber engineer github information steeled by key logging then break into Uber AWS account	Uber	Anonymous	2017	**57 M Driver's credentials steeled, $100000 Paid to Hackers**
9.	Anthem	Trojan containing key logger	Anthem Corp.	Chinese Group	2015	**80 M Patients Information stealed**
10.	Sony Breach	Social engineering, phishing mails with key logging malware	Sony Pictures	Guardians of Peace	2014	**$100 M Loss**
11.	Target Card	Card Skimming malware	Target	Anonymous	2013	**70 M Credit card Info.**

5. CONCLUSION

The survey conducted in this paper mainly focuses on three abstruse attacks that are key-logging Trojan horse, Sim cloning, and RFID theft in banking transactions. To prevent data breaches caused by such attacks, organizations and individuals must be aware of such types of attacks. One must use the anti-virus software to scan systems periodically for any foreign

material. The live survey mentioned in this paper has shown the severity of cyber-attacks and it has also shown how these attacks impact globally. It also proves the seriousness of having cyber security in organizations. The author has found out the undiscovered areas in research by surveying numerous research papers. This literature survey has shown that the advanced version of key logger is not yet detectable by any standard anti-virus software and windows defender. The majority of Sim cards operate on the basic encryption algorithm which is comp128, this algorithm is vulnerable to physical Sim cloning. When the Sim card is in a roaming service network, the information that needs for authentication is exposed on the air through which hackers can manage to obtain encryption keys which leads to OTA Sim cloning. Credit cards containing RFID tags can be accessed through an RFID tag reader by an attacker. This study has revealed the research gaps and the flaws in the existing systems. In the future, research will be conducted to minimize the flaws mentioned above as well as to protect the digital systems from a data breach.

REFERENCES

[1] Dr Akashdeep Bhardwaj, Dr Sam Goundar , ELSEVIER,Keyloggers:silent cybersecurity weapons,Volume 2020, Issue 2, February 2020, Pages 14-19,10.1016/S1353-4858(20)30021-0.

[2] Huseyn Huseynov,Kenichi Kourai,Tarek Saadawi,Obinna Igbe,Virtual Machine Introspection for Anomaly-Based Keylogger Detection,2020 IEEE 21st International Conference on High Performance Switching and Routing (HPSR) ,2020,10.1109/HPSR48589.2020.9098980

[3] Jia Wang, Brent Lagesse,KeyGuard: Using Selective Encryption to Mitigate Keylogging in Third-Party IME ,2020,arXiv:2011.10012

[4] Ahsan Wajahat; Azhar Imran; Jahanzaib Latif; Ahsan Nazir; Anas Bilal,A Novel Approach of Unprivileged Keylogger Detection,2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET),IEEE,25 March 2019,10.1109/ICOMET.2019.8673404

[5] Yazeed Albabtain; Baijian Yang,The Process of Reverse Engineering GPU Malware and Provide Protection to GPUS, 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE),IEEE,06 September 2018, 10.1109/TrustCom/BigDataSE.2018.00248

[6] Nikhil Tekawade; Shruti Kshirsagar; Shripad Sukate; Leena Raut; Shubhangi Vairagar,Social Engineering Solutions for Document Generation Using Key-Logger Security Mechanism and QR Code,2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA),IEEE, 25 April 2019,10.1109/ICCUBEA.2018.8697420

[7] Darshanie Sukhram; Thaier Hayajneh,KeyStroke logs: Are strong passwords enough?, 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON),IEEE,08 January 2018,10.1109/UEMCON.2017.8249051

[8] Adam Prayogo Kuncoro; Bagus Adhi Kusuma,Keylogger Is A Hacking Technique That Allows Threatening Information On Mobile Banking User, 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE),IEEE,2019,10.1109/ICITISEE.2018.8721028

[9] Arun Pratap Singh; Vaishali Singh,Infringement of Prevention Technique against Keyloggers using Sift Attack,2018 International Conference on Advanced Computation and Telecommunication (ICACAT),19 December 2019,IEEE,10.1109/ICACAT.2018.8933805

[10] Danial Javaheri; Mehdi Hosseinzadeh; Amir Masoud Rahmani,Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines,IEEE Access (Volume: 6),07 December 2018,IEEE,10.1109/ACCESS.2018.2884964

[11] C. Occhiuzzi(1,2), S. Amendola(1,2), S. Nappi(1,2), N. D'Uva(2) and G. Marrocco(1,2) RFID Technology for Industry 4.0: Architectures and Challenges,181-186, IEEE 2019 https://doi.org/10.1109/RFID-TA.2019.8892049

[12] 1Ag. Asri Ag. Ibrahim, 1,2Kashif Nisar, 1Yeoh Keng Hzou, 2Ian Welch, Review and Analyzing RFId Technology Tags and Applications, IEEE 2019, https://doi.org/10.1109/AICT47866.2019.8981779

[13] Xiulong Liu Xin Xie Xibin Zhao Keqiu Li Alex X. Liu Song Guo Jie Wu, Fast Identification of Blocked RFID Tags, (Volume: 17, Issue: 9Sept. 1 2018), https://doi.org/10.1109/TMC.2018.2793219

[14] Dr. Harman Preet Singh Department of Management & Information Systems, College of Business Administration, University of Hail. EXPLOITING RFID FOR BUSINESS TRANSFORMATION: A STRATEGIC ANALYSIS VIS-À-VIS AGRICULTURAL BANK OF CHINA, Volume : 5 | Issue : 1 | Jan 2019

[15] Mugahid Omer1, Yachao Ran2, and Gui Yun Tian1, 2, Indoor Localization Systems for Passive UHF RFID Tag Based on RSSI Radio Map Database, Progress In Electromagnetics Research M, Vol. 77, 51–60, 2019

[16] Roben A. Juanatas, Irish C. Juanatas RFID-Based Library Management System with Android Mobile Access Application, December 11–12, 2019, Amity University Dubai, UAE, 978-1-7281-3778-0/19/$31.00 ©2019 IEEE

[17] Arvind Lakshmanan , Vivek Maik SRM Institute of Science and Technology, Active RFID Tag with Better Tracking Range for Automotive Applications IEEE 2019

[18] Meryle Mvoulabolo1, Tebello N.D. Mathaba2, Marcel O. Odhiambo3, Performance analysis of binary search based RFID anti-collision algorithms May 08,2020

[19] Weiping Zhu∗, Mingzhe Li∗, Jiannong Cao†, Zongjian He‡ and Rong Xie∗§, Multiple Resolution Bit Tracking Protocol for Continuous RFID Tag Identification, 2019 IEEE
[20] Oussama Boularess, Taoufik Aguili , Jawad Yousaf Department of Electrical and Computer Engineering , Design of Robust Detection System for Printable Chipless RFID Tag Alphabet Letters , 978-1-7281-4064-2019 IEEE
[21] N. Zidouni, S. Chitroub, H. Chebout and N. Boukais, "New safety measure to protect the 3G/4G SIM cards against cloning," 2018 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), 2018, pp. 1-8, doi: 10.1109/MoWNet.2018.8428876.
[22] https://cyware.com/news/understanding-sim-swapping-and-cloning-attack-techniques-230934eb
[23] https://securityintelligence.com/posts/clone-or-swap-sim-card-vulnerabilities-to-reckon-with/
[24] https://www.infosecawareness.in/concept/sim-swapping-and-sim-cloning-frauds?lang=en
[25] https://www.archclearing.com/News/News/11594/SIM%20Cloning.xhtm
[26] https://www.makeuseof.com/tag/ways-sim-card-hacked/

BIOGRAPHIES

Prof. Vina M. Lomte
Project Guide and Head of Computer Engineering Department at RMD Sinhgad School of Engineering, SPPU, Pune.

Mr. Shubham S. Patil
Project Team Lead and B.E. Student at Department of Computer Engineering, RMD Sinhgad School of Engineering, SPPU, Pune.

Ms. Anuja Lokhande
Project Research Fellow and B.E. Student at Department of Computer Engineering, RMD Sinhgad School of Engineering, SPPU, Pune.

Mr. Kartik Mogal
Project Research Fellow and B.E. Student at Department of Computer Engineering, RMD Sinhgad School of Engineering, SPPU, Pune.

Ms. Komal Mohite
Project Research Fellow and B.E. Student at Department of Computer Engineering, RMD Sinhgad School of Engineering, SPPU, Pune.