International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Privacy Risks and Security Practices in Digital Technologies

S.Karunakaran, A.Sivakumar, N.T.Renukadevi, K.Saraswathi

Abstract— Digital Technologies are getting worldwide popular. People are bounded with emerging technologies to make their life faster and smarter. Business organizations over the world taking this as an opportunity to launch more digital products to cover people. Users not aware of the importance of their private data. But the others know how to make use of it in favor of them. People need to be conscious and tailored to life in the digital age. This paper reveals the technical loop holes in variety of current digital applications that are familiar among the people. The aim is to create awareness among the people on security practices to safeguard from digital attacks.

Keywords : Privacy, Security, Google, Facebook, Whatsapp, Torrent.

I. INTRODUCTION

With the explosion of networked electronic communication came off-putting capabilities to gather, process, merge and store data, resulting in previously unseen transformational force on the concepts of trust, security and privacy[1][2]. The Internet in future will bring about a globe where authentic life will incorporate physical and digital life[3]. Trust and identity stretch out at the basis of numerous human connections and transactions, and societies have developed genuine worry for privacy being vital for liberty and inspiration[4].

The capability to control the release of personal information is a essential factor for establishing levels of faith in society. Privacy has lots of aspects, it tell about culture, history, ethics, the location of individuals in society, public and private safety, legislation, economics, technology etc.[5] In several societies it is a significant concern at the base of societal values, in particular for sustaining autonomy and the ability to exert democratic rights and human independence[6][7]. The concept of privacy is theme to change over time. It is related to cultural. The challenges created by the rising digital world require urgent concentration. We may currently observe the most enormous and intense transformational heaviness in known human history on the perception of privacy[8]. It is necessary therefore to work towards overcoming these social characteristics into the digital space[9].

II. DIGITAL TRANSACTIONS

Nowadays the usage of debit card and credit card for online digital payments becomes trendy. We have no time to be aware of the security concerns with these transactions. Only few frontend servers like Amazon, Google are concentrating about user privacy[10]. But there are good number of portals which are used by people frequently never care on user privacy.

In most of the online payments, during the first time transaction the user card details are stored in the server buffer and the same may be prefilled during the subsequent payments in that portal. The user only needs to enter the Card Verification Value (CVV) number. There is possibility of stealing user account details if the security features of these servers are weak.

A. NFC Cards

Presently card swipe machines are used in POS terminals to process payment transactions. It is a time consuming process and also the scratches in magnetic strip of the card may lead to delay or rejection in processing. Sometimes the payments are deducted more than one time.

Fig1. NFC Reader

To overcome this, contactless Near Field Communication (NFC) card were introduced. The processing time of this type of card was quicker, since the user only needs to tap the card over the POS machine enabled with Radio-Frequency Identification (RFID).

Manuscript published on November 30, 2019.
* Correspondence Author
Dr.S.Karunakaran*, AP/Computer Technology, Kongu Engineering College College, Perundurai, Tamilnadu, India. (Email: karunakarankrs@gmail.com)
Dr.A.Sivakumar, AP/Mechanical, Kongu Engineering College College, Perundurai, Tamilnadu, India.(Email: askmech@kongu.ac.in)
Dr.N.T.Renukadevi, AP/Computer Technology, Kongu Engineering College College, Perundurai, Tamilnadu, India. (Email: renuka@kongu.ac.in)
Dr.K.Saraswathi, AP/Computer Technology, Kongu Engineering College College, Perundurai, Tamilnadu, India. (Email: saraswathik@kongu.ac.in)

Some banks allow the user to configure their card in such a way that, up to certain limit the payment was authorized without pin number. This enables some fraudulent to carry the NFC readers nearby the person who was possessing NFC card and make payments without his knowledge.

B. Google

Amazon alexa is an Internet of Things (IOT) enabled device which can recognize our oral commands and act accordingly. These conversations may be monitored and stored in Amazon database. Stored data may be used in future for commercializing users' private interests.

Our day-to-day activities are highly linked with Google services. Searching, email, drive docs, contacts, Google pay, YouTube, Play store. everyone in the world associated with at least one of the said Google tools every day. For accessing these tools we login with Google. We keep always log in feature and store our password in cookies for faster login. Most users are not aware of the problems associated with this. Google is introducing new features and techniques to people every often. We are also using these features without any payment. We never think of how come Google business runs profitably and their market shares are in rise. User personal data collected from different Google services are marketed by Google. An organization only running with our data alone have become such a financially sound giant organization in the world. Just imagine the worth of our data.

https://myactivity.google.com reveals our activities with Google services. We can use this services to conform that our account was not misused by others.

But at the same time, if our Google username and password available with someone else that can be used by them to monitor and misuse our activity log. If anyone who knows my account details can get my personal data, you just think what else admin can do with these data.

C. Keyboard

We use physical keyboard in our laptop and desktop for entering data. While entering secured information like username, password and pin in real keyboard there is a potential possibility that our keystrokes can be recorded and misused by hackers. Hacking script like key logger may be installed in our system without our knowledge [11]. Then it started to capture our key strokes. Hackers can access these key logs over network.

D. WhatsApp

It has become one of the family members whom we often communicate. We use it for public and private conversation. WhatsApp says our conversations are secure. When we delete our private conversation, we think that data erased from everywhere. But it was not fully true. Even after you erase, all deleted conversations can be accessed using .crypt12 file and WhatsApp key. Taking backup of your conversations in Google makes it more vulnerable.

E. TrueCaller

Truecaller is used for identifying the exact person of the communication to keep protected from spam and other fraudulent. We all believe true caller always true to us.

But sometimes it was false to us. We give permission in our mobile for Truecaller to access our SMS and contacts. This enables them to track our contacts and read the read our SMS conversations including our One Time Password (OTP) without our knowledge.

F. Payment Apps

As many countries are interested in cashless transactions, payment apps are highly demand in the market.

Fig2. Payment App

Instead of paying with cash, cheque, or credit cards, a customer can use a mobile to pay for a broad range of services. They made pin verification for all financial transaction initiated by the user. They also offer cash rewards for our payments. People think that they give money from their packet for using their product. But the truth is different. They deduct charges in our bank account linked with them for maintenance, Unified Payments Interface (UPI), processing fee etc., these deductions are made without our knowledge and pin verification.

Unless and otherwise you go through your complete bank statement on regular basis, it was hard to find them. We have to understand that payment apps have full control of our bank account; they can access our account at any time.

G. Facebook

Popular social media in the world, where people used to share all their feeling in their life. People can find many online friends and join group of their interest. People post their personal information to get more likes without caring of privacy. Unfortunately there are many fake accounts exists. Facebook continually monitor and analyze our posting to track our feeling. They prioritize the posting order based on our feelings.

By reading a Facebook page of an individual we can judge the character and personal interests of any individual. Facebook also show situational advertisement by tracking My page history. Messages and photos can be accessed by unauthorized person and it may used as a tool to threaten them.

H. Torrent

It is a file download concept in which instead of a single server, a file split into many pieces and downloaded from multiple servers at same time.
Using Bit Torrent protocol.

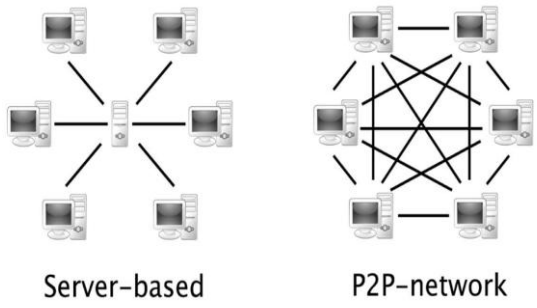

Fig3. Torrent Network

Advantages:-

- High Efficiency
- Easy sharing
- Prevents broken files from sharing
- Reduce upload/download time

Disadvantages:-

- Seeder can only seed one (or) two files at a time
- Computer performance may drop
- Unpopular files are hard to find

Currently this protocol concept is misused by unauthorized persons to share valuable files like Operating system, Movies, licensed software. Due to this digital way of sharing high financial loss incur for the proprietor of the organization. Identifying from which server seeding initiated was a difficult task. Once it started to spread it was not possible to control the sharing. Discovering the person and location beyond the attack was not technically feasible.

I. Darkweb

Publically available web services are averaging only 10% in the world. About 90% web services are not known to common people[12]. (Internet Service Provider) ISP can track only limited public web services. But the remaining web services in the dark side of the internet are out of control from ISP. These services are called 'onion sides', since their origin cannot be tracked.

They can be accessed using 'tor' browser. These web services are used for selling of illegal drugs, weapons, electronics, hacking tools etc., all over the world without any regulation. The transactions are unanimous and payment made through Bitcoins and crypto currency.

J. Radiofrequency

Wireless transactions of data are more convenient nowadays. But in the other side it also convenient for the Hackers to steel data without our knowledge. One can hack something even not visible to the eyes. Devices like 'HackRF1'are readily available in the open market which can be used for access of radio frequencies.

Fig 4. Radio Frequency Hacker

Entire operation of a car and control of devices within the car can be illegally accessed by the attackers. Walkie-talkie conversations can be tracked to control decisions and create financial loss

III. SECURITY PRACTICES & RESULTS

Table-I: Potential Risks and Resolving Practices

Digital Technology	Privacy Risk	Security Practices
NFC Card	Unauthorized Payment	▪ Never allow any payment in NFC card without PIN verification. ▪ Aluminium foil type cover can be used to protect your card from illegal access
Google Services	User Tracking	▪ Ensure that you have enabled don't track me in user private setting ▪ Two way user authentication ▪ Don't let Google always log in option
Keyboard	Recording the keys	▪ Use virtual keyboard for entering secured information like Password and PIN ▪ Track task manager to check installed programs
WhatsApp	Loss of Private Chats	▪ Remove .crypt12 files from WhatsApp database frequently ▪ Don't allow for Google Backup
True caller	Hammering of SMS conversations	▪ Avoid using true caller to the extend ▪ Regulate your permissions

Payment app	Unauthorized debits	▪ Ensure PIN verification is must for all payment transactions including admin initiated transactions ▪ Biometric authentication ▪ Reduce using multiple payment gateways
FaceBook	User Privacy	▪ Care must be taken before accepting friend requests ▪ Think before sharing data in public
Torrent	Illegal File sharing	▪ Ethical values
Dark web	Criminal worldwide Transactions	▪ Tight ISP regulations ▪ Verify URL
Radio frequency	Information Theft	▪ Dynamic Security code generation ▪ Avoid using public Wi-Fi

IV. CONCLUSION

Digital technologies have become obvious part of our daily life. In variant of profession everyone around the world connected with digital services many a times in a day. As the coin has two sides, digital technologies are not missing from security concerns. Especially considering user privacy, the worth of the data and its business opportunities make it more vulnerable. Weakness in common technological services around us has been revealed here. This study highlighted significant insight on the different current issues connected to security threats on the digital environment and propose certain solutions for tackling these security concerns. The findings reveal the benefit of thinking about security in the wider sense. Certain technological risks and the security practices to resolve it has been tabulated above. These solutions are marginally reasonable for high-level security necessities. It's a good practice for users to adhere digital security guidelines in order to protect themselves from attacks. The existing security solutions are required to be enhanced upon, due to the rising potential of attackers and growing risks with the popular digital technologies.

REFERENCES

1. Dirk van Rooy and Jacques Bus "*Trust and privacy in the future internet—a research Perspective*", Springer 2010, IDIS (2010) 3:397–404,DOI 10.1007/s12394-010-0058-7.
2. Tariq Ahamed Ahanger and Abdullah Aljumah "*Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms*" , IEEE Access 2019, P.no.11020-11028, DOI: 10.1109/ACCESS.2018.2876939.
3. S. Bradner, "*Internet privacy conflicts*" Network World, 27 (18) (2010), p. 15.
4. J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos,"*Security and privacy for cloud-based IoT: Challenges*," IEEE Commun. Mag., vol. 55, no. 1,pp. 26 33, Jan. 2017.
5. Nir Kshetri "*Privacy and security issues in cloud computing: The role of institutions and institutiona*l", Elsevier Telecommunications, Volume 37, Issues 4–5, May–June 2013, Pages 372-386.
6. Mark Burdon A,Lizzie Coles Kemp, "*The significance of securing as a critical component of information security: An Australian narrative*", Elsevier Computers & Security Volume 87, August 2019, pp.1-10.
7. Albrechtsen, E and Hovden, J "*Improving information security awareness and behaviour through dialogue, participation and collective reflection. An interven- tion study*" Comput. Secur. 29 (4), 432–445. DOI: 10.1016/j.cose.20 09.12.0 05.
8. Spears, J.L., Barki, H.,"*User participation in information systems security risk management*" MIS Q. 34 (3), 503–522. DOI: 10.2307/25750689.
9. Kolkowska, E and Dhillon, G "*Organizational power and information security rule compliance*" Comput. Secur. 33 DOI: 0.1016/j.cose.2012.07.001.
10. Chipperfield, C and Furnell, S. "*From security policy to practice: sending the right messages*" Comput. Fraud Secur. 2010 (3), 13–19. DOI: 10.1016/S1361-3723(10) 70025-7.
11. E. Albrechtsen "*A qualitative study on users view on information security*" Comput. Secur., 26 (2007) (2007), pp. 276-289.
12. P. Balozian and D. Leidner "*Review of IS security policy compliance: toward the building blocks of an IS a security theory Data Base*" Adv. Inf. Syst., 48 (3) (2017), pp. 11-43.

AUTHORS PROFILE

Dr. S. Karunakaran was born on March 15, 1979 in Erode. He received B.Sc., Degree in Computer Science from Nagamalai Navarasam Arts and Science College, Bharathiar University, Coimbatore, TamilNadu, India in 1999; Master of Computer Applications degree from Kongu Engineering College, Bharathiar University, Coimbatore, India in 2002 and M. Phil., degree in Computer Science from Manonmaniam Sundaranar University, Tirunelveli, India in 2003; Ph.D in Computer Science from Anna University Chennai in 2012. He became member of IEEE in 2007. Presenly, he is working as an Assistant Professor (SRG), in the School of Computer Technology and Applications, at Kongu Engineering College, Perundurai, Erode, Tamilnadu, India. He has been in the teaching profession for the past 16 years. He has guided 8 post graduate projects and 34 under graduate projects over these years. He has published 10 papers in International Journals, 12 papers in International Conference and Presented 21 papers in National Conferences. His academic interests include ad-hoc networks, distributed computing and wireless communication.

Dr.A.Sivakumar working as full-time faculty member of Mechanical Engineering Department in Kongu Engineering College (Autonomous) affiliated by Anna university Chennai at Perundurai TamilNadu. Did his postgraduate and research at NIT Tiruchirapalli. Specialization is Engineering optimization and industrial Engineering. Published 13 international journal and 22 international renowned conferences conducted by IITs, IISc, NITIE, IIMs and NITs. Actively involved in sponsored projects funded by UGC. Current fields of interest are engineering optimization, maintenance policy and artificial intelligence. Member of IIIE,MISTE and fellowship in Institution of Engineers (India) -FIE.

Dr.N.T.Renukadevi received the M.C.A and M.Phil Degrees in Computer Science from Bharathiar University, India in 2003 and 2008 respectively. She received Ph.D. degree in Computer Applications from Anna University, India in 2014. Since 2008, she is working as an Assistant Professor in the Department of Computer Technology, Kongu Engineering College. Her research interests include Data Mining and Image Processing. She is also reviewer in reputed journals.

Dr. K.Saraswathi received the M.Sc., and M.Phil Degrees in Computer Science from Bharathiar University Coimbatore, India in 2004 and 2006 respectively. She received Ph.D. degree in Computer Applications from Anna University, India in 2018. Since 2008, she is working as an Assistant Professor in the Department of Computer Technology, Kongu Engineering College. Her research interests include Data Mining and Opinion mining.