IEIE Transactions on Smart Processing and Computing

Privacy and Security Data-sharing Technologies for Tampering Protection and Detection

S. M. Buddhika Harshanath

Department of Software Engineering, Faculty of Computing, Sri Lanka Institute of Information Technology,
New Kandy Road, Malabe, Sri Lanka hasrshanath.s@sliit.lk

Received December 30, 2018; Accepted January 25, 2019; Published February 28, 2019

** Regular Paper*

Abstract: Digital transformation enables the development and testing of available applications for customer use, done in a smart way. It is also clear that the vast amounts of available data related to business cannot be easily handled in a day without the use of these mobile resources. Yet, privacy and security factors affect the release of more data for publishing or exchange. Open data is ruled out due to insufficient available data for research, as related to mobile devices, where there is a need for real data sets for testing purposes. The Internet of Things demands stronger security mechanisms to keep attacks in buildings and automobiles at bay. However, it must not be ignored that rules and regulations require considerable time to come into effect, whereas self-control, imposed by a user made aware of the risks, takes little or no time at all.

Keywords: Mobile computing devices, Social networks, Control, Privacy and security, Social network services

1. Introduction

Sri Lanka, on its way to global business, realizes the value of the use of mobile devices for connectivity, communications, and the conduct of business from anywhere, anytime. This, in turn, has helped productivity levels to increase. However, there are issues related to the release of necessary information in this manner. There is hardly any, or no, guarantee on the security of released data. Data sharing, as everyone knows, is an essential and indispensable commodity in a fiercely competitive business environment. As such, maintaining the security of an organization's available data adds distinctive value to its organizational culture to inform and influence employee behavior.

Information security is the key to a set of internal controls governing the processes, operations, and transactions in an organization. Information security is a prerequisite of business processes. Furthermore, information security adds distinct value within the institutional culture towards keeping employees informed and, where necessary, influenced. Therefore, it is essential that these controls be internalized so that individuals are directed towards protecting valuable information. If not done, the organization, or an individual, is likely open to potential harm. Employers permit social networking at work for various reasons. They may need to register for certain social networking sites (SNSs), and sometimes, there is an SNS for use internally in a particular enterprise [1]. Over the years, data mining and privacy have generated much thought towards the enhancement of privacy. Models, measures, methods, and technologies have surfaced aimed at protecting sensitive information [2]. However, the advent of big data poses a huge challenge to the field. This paper considers some such challenges. It also suggests new lines of research to meet the challenges.

It is globally accepted that the use of mobile devices accelerates the communication demands of the modern day, besides making tasks more convenient for users. In such a scenario, the increased use of mobile devices in business reveals an increase in employee productivity [3]. According to a recent Aberdeen study, the best-in-class enterprises enjoy a 40% increased productivity rate [4]. Fig. 1 offers global and local digital-use snapshots. Mobile connections are exceeding the percentages worldwide.

Digital transformation, on the other hand, is about innovations to existing applications with the initiative to promote faster competition among business interests constantly on the lookout for more personalized, always available, digital customer experiences. The hunt is on for further adoption and specializations in communications or content. Facebook, however, will represent a common denominator to all companies, as shown in Fig. 2. There is reason to believe that the pressures of using the social networks prevalent in developed countries could appear elsewhere as well.

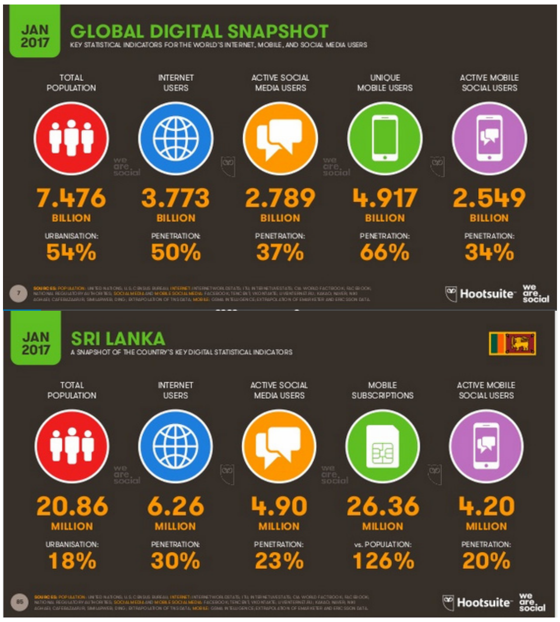

Fig. 1. Digital use in 2017: global vs Sri Lanka [5].

Tech companies like Facebook, Google, Apple, and Amazon have already made their way into personal and social interactions seeking more information about us. Privacy violations in cyberspace are now commonplace. The international airline Emirates was virtually handing over customers' sensitive information to marketers and hackers, according to one data security engineer. "The moment you click on Manage Preferences to select a seat or meal for your trip, or to check in to your flight, your booking ID and last name is passed on to approximately 14 different third-party trackers, like Crazy egg, Boxever, Coremetrics, Google, and Facebook, among others" [6].

It is known that some websites automatically collect information about users. Cookies and web beacons allow collecting of information. Cookies stored by the computer's Internet browser may be accessed and recorded by other websites visited, but do not execute code or access other stored information. Web beacons are transparent pixel images used for collecting information about website usage, e-mail responses, and tracking [7].

Information that may be collected by cookies when using websites may include, without limitation, the following:

1. The pages visited within the site; the date and time, and the time spent using it.

2. The computer and connection information, such as the IP address, browser type and version, operating system, and platform.

Access to sites through a mobile device may also help identify its location. Perhaps the user might not like this idea, and will adjust location details by adjusting the mobile device's location services settings. This can be done by contacting the service provider or device manufacturer for instructions on changing the relevant settings. The information automatically collected may be used to enhance the performance of these websites.

The Information Systems Audit and Control Association (ISACA) claims to be using location information (if shared with ISACA) to identify the geographic locations from which content is accessed. This, apparently, is a move to better understand what content topics may be most relevant in those regions, and to help ISACA members generally to develop resources around those content topics [7]. However, the absence of a control for physical devices, with employees using personal devices for business/personal use in the office, has helped increase mobile-device risk levels [8, 9]. Therefore, it is imperative, when deploying such tools, to consider the potential benefits, risks, and controls associated with the technology.

Table 1. Survey results [10].

Question	Positive Responses (%)	Total Responses
Use a computer and/or mobile computer device	72.50	400
Login account at office	53.75	400
Official email account	55.26	380
Getting unofficial email to your official email	72.37	380
Sharing the resources with others	52.63	380
Embarrassed by revealing incidental information to others	60.81	370
Prefer privacy & security at office	75.00	380

A survey on the use of communication devices by workers reveals the information shown in Table 1. The questions are related to the type of use.

This information helps enhance site performance and user experience. For an employee, it is necessary to know about the importance of security, about the dependence on others to take responsibility, and that the refusal to accept personal responsibility for security (because it could be too technical) may contribute towards security threats. Internationally, such studies are constantly done. But in Sri Lanka, very few are done. According to a survey conducted among some 400 office workers, almost 72.5% of workers use a computer and/or mobile device at work, and 72.27% enjoy an e-mail facility and/or social networks. But they exhibit a lack of security measures when using mobile devices with their social networking and e-mail accounts. Some of them had even lost their mobile phones and or mobile devices. Table 1 gives details about the research, with 75% responding that they prefer privacy and security in the work place, which we cannot expect [10].

Sensors, cyber–physical systems, smart mobile devices, social networks, the Internet of Things (IoT), and smart and connected health care promote the capture, processing, and sharing of big data [11] for useful information, such as patterns and to predict trends and events [12].

Mobile devices enable individuals and enterprises to have valuable experiences. *The Economist* claims that well-managed data could be sources for new economic value, enabling further exploration, with science while holding governments accountable [13]. Yet, the technologies need careful management to avoid

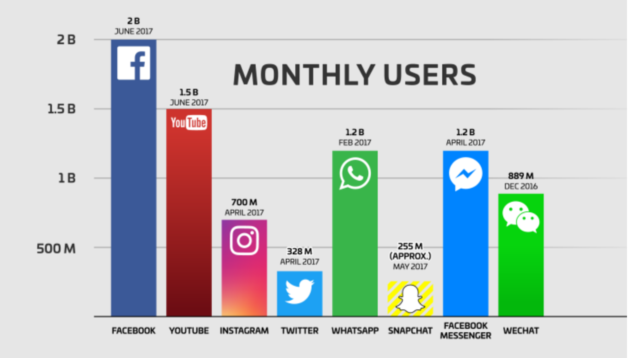

Fig. 2. Major Social Media Platforms [26].

unnecessary risks in order to maintain value.

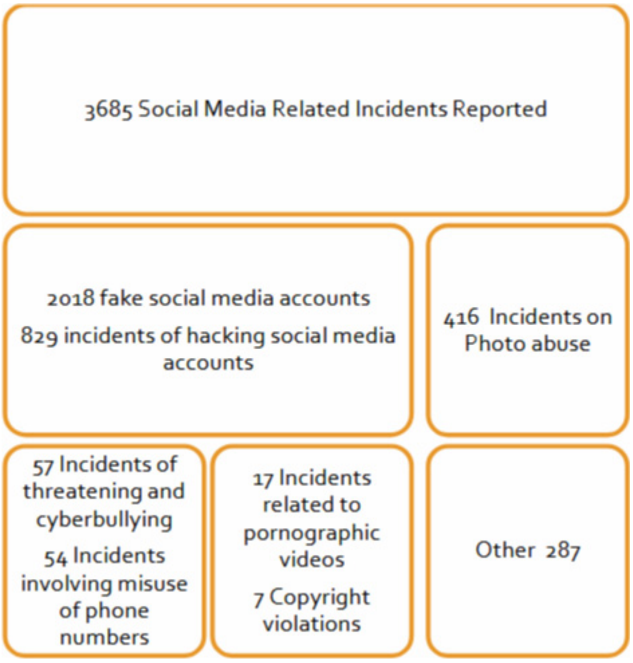
3685 Social Media Related Incidents Reported
2018 fake social media accounts
829 incidents of hacking social media accounts
416 Incidents on Photo abuse
57 Incidents of threatening and cyberbullying
54 Incidents involving misuse of phone numbers
17 Incidents related to pornographic videos
7 Copyright violations
Other 287

Fig. 3. Some statistics about people involved in "digital government" according to the incidents reported [14].

2. Risk and Security Concerns

Mobile devices are open to malicious as well as internal, non-malicious threats. Portability, the best advantage of mobile devices, could also be the biggest threat. Mobile devices use wireless networks to transport data. Information that travels across these networks is said to be less secure than traveling wired networks, because it can be intercepted and captured. That can affect reputations, and may even require legal action. Lost data can also affect production in an enterprise or organization.

Many mobile devices can store data; leaving data unencrypted result "unprotected" data. Information gathered in this manner from the interception of data in transit or from the theft or loss of a device can compromise the security of sensitive and proprietary information. Mobile devices can also introduce malware and can become platforms for other malicious activities. Devices and laptops with onboard microphones, and cameras in particular, are vulnerable because those components can easily be activated using publicly available tools, propagating malware, data loss, and eavesdropping. Similarly, cellular and voice-over-IP technologies have vulnerabilities that make it easy to exploit intercepted calls. However, protection from some threats requires additional layers of protection, with technical controls and countermeasures such as encryption and third-party security software.

For the past six years there has been a rapid increase in cybersecurity-related incidents reported to the Sri Lanka Computer Emergency Response Team and Command Center (SLCERT/CC) [14], as shown in Table 2. According to the information shown, reported incidents rose from 71 in 2010 to 222 in 2017. The number of reported social media–related incidents has also increased exponentially, ballooning from 80 incidents in 2010 to 3685 incidents in 2017.

Yet, employees need motivation to adjust their behavior. The first task, therefore, is to raise awareness and convince staff about the personal stakes involved in information security for an organization's information assets. It is apparent that some known vulnerabilities and associated threats already exposed need to be understood and attended to when dealing with mobile devices. Information can become uncontrollable with misleading or false details spread through social media [5, 26]. The restrictions were imposed by the government and resulting unauthorized accesses in order to gain access. Then, systems become vulnerable and can suffer huge losses. For example in 2018, Sri Lanka was forced to restrict the use of some social media services [16], after many people with little or no knowledge of virtual private networks (VPNs) [15] allowed access to restricted networks [16] by intruders spying on mobile communications and conducting forensic analysis of seized phones. Although VPN services are widely in use, their operational transparency and likely impact on user privacy and security concerns remain.

Android app developers benefit from native support to implement VPN clients via VPN permissions to provide censorship circumvention, support enterprise customers, and enhance online security and privacy. However, despite the fact that Android VPN-enabled apps are installed by millions of mobile users worldwide, their operational transparency and their possible impact on user's privacy and security remains "terra incognita" for even tech-savvy users [17, 26].

Private communications providers have acted as physical and legal gatekeepers, separating government and individuals' communications, ensuring that the appropriate process is followed before providing access to data and services. Physically, a handover interface must serve data to the requesting government entity in order to provide access for lawful surveillance [18]. Legally, companies are the custodians of their customers' data. They receive a request for data and hand them over to the appropriate government agency [19] the procedure is illustrated in the Table 4.

Table 2. Increased computer crime, per SLCERT/CC [14].

Incidents Types	2012	2013	2014	2015	2016	2017
Phishing	08	08	12	14	23	42
Abuse/Privacy Violation	08	08	08	21	32	29
Scams	06	18	12	18	12	32
Malicious Software/ Ransomware	02	02	03	12	21	39
Financial Frauds	-	-	-	10	16	35
Compromised Websites	15	16	56	20	10	25
Compromised Emails	06	08	10	16	16	14
Intellectual Property Violation	03	03	03	03	07	06
Unauthorized Access	01	11	08	-	-	-
DoS/DDoS	01	01	06	03	04	-
Social Media Incidents	1100	1200	2250	2850	2200	3685

Table 3. Available mobile security apps for security of data.

App	Details
Orbot	The best way to browse privately on an Android device is to use Tor's application called Orbot, a free proxy that uses Tor to encrypt Internet traffic and reroute it though computers around the world. The app is available for Android 4.0 and above. Users with older versions will need to manually download the app from the Guardian Project website.
LastPass	One simple way to stay safe is to change passwords. This can be confusing because every password for each document has to be remembered. LastPass does the hard work remembering everything. All data are encrypted, so the app keeps the information safe and allows entry into favorite sites with one click.
Find Your Phone	Find Your Phone is a new feature on Android. By searching with the string “find my phone” on any browser through Google website, it is possible to locate the phone, lock and call it, secure accounts, and leave a callback number on the screen for the person who finds it.
My Secure Mail	My Secure Mail is a universal email client. It allows people to manage an unlimited number of mail accounts from various providers. My Secure Mail keeps all emails in one place and ensures they are safe using encryption and password-protected sign-ins.
NordVPN	NordVPN is for those who have not used a VPN before. It helps keep all online activity private by encrypting all the data coming in and out of the device and securing all Internet traffic. The NordVPN Android app reroutes and encrypts all Internet traffic to make the connection private and secure, and is an alternative to Tor's Orbot.
Signal	The encrypted messaging and voice-calling app Signal is a sure-fire way to communicate safely on an Android device. It provides end-to-end encryption to secure all communications, and the app can also verify the identities of those who are messaging. It also verifies the reputation of the channels used.
Tor Messenger	Tor Messenger is somewhat similar to Signal and is a safe and encrypted way for private conversations. It is a cross-platform chat app, secure by default, and sends all messages over the Tor Network. The ChatSecure app also allows sending communications across Tor.

3. Strategies to Address Risk Associated

The Google-owned Android operating system is currently the largest in the world based on the number of users. Nevertheless, many users may not be using the latest versions, which fix bugs and eliminate vulnerabilities. Perhaps Google will eventually force Android users to update the operating system to the most recent version to help them be more assured about privacy [20]. Table 3 explains some secure apps and their details.

The browser may be customized to reject cookies or to inform the user about them beforehand. A good anti-virus protection app on a smartphone does not necessarily mean complete security, because mobile device security is comprised of security for different features, such as data privacy and security features, permission restrictions against snoopy apps, and a blacklist for undesired calls. It is advisable to have an Excellent backup capability, in case of deterioration of the smartphone, in addition to encryption functionality. A holistic security management program for the protection of mobile devices should become a key part of the overall security governance. The program for protection of mobile devices should ensure multilevel security for usage of such devices.

4. Governance and Change Issues

Deploying mobile devices is not a technical activity alone. It affects the daily operations of employees and organizational information flow towards the business processes of the enterprise from many perspectives. Using mobile devices may slow down the daily tasks of a user due to communication problems. They may even put corporate information at risk, affect daily operations, impact existing elements of the technical infrastructure, or be affected by external factors. VPN apps from Google Play present several limitations, many of which are

Table 4. Managing mobile devices and relevant framework procedure [19].

Challenge	Control	Relevant ISACA Framework* Processes
A lost or stolen mobile device	Implement a central management console for device remote ontrol—i.e., location tracking, data wipe-out, password/PIN change or user strong authentication.	**COBIT DS5** **Risk IT RR3**
Enforcing the enterprise policy for standard devices	Gain visibility of all devices connected to the infrastructure.	**COBIT PO1, PO6, DS5** **Risk IT RR2**
Providing support for various devices	Turn to cross-platform centrally Managed mobile device managers.	**COBIT DS5** **Risk IT RR2, RR3**
Controlling data flow on multiple devices	Secure the systems that are accessed with authorization, encryption and Privileges control.	**COBIT DS5, DS11** **Risk IT RR2**
Preventing data from being synchronized onto mobile devices in an unauthorized way	Monitor and restrict data transfers to handheld or removable storage devices and media from a single, Centralized console.	**COBIT DS5, DS11** **Risk IT RR2, RR3**
Keeping up with the usage of the latest and greatest devices	Create keen user awareness of Information assets, risks and value.	**COBIT PO6** **Risk IT RR1, RE3**
Promoting accountability, responsibility and transparency with device usage	Track the way devices are used and provide regular feedback to Management.	**COBIT PO4, ME2** **Risk IT RR1**

inherent to static and dynamic analysis [21].

Introduction of mobile devices in an enterprise serves the corporate strategy and objectives, and needs to utilize a proven framework, such as Control Objectives for Information and Related Technology (COBIT) [22]. The chosen framework should encourage user-feedback mechanisms from all levels of the organizational hierarchy in order to identify possible side effects in a timely manner and to respond accordingly.

It is easy to share a link to a website and get a friend's attention. But is there a guarantee that other users are paying attention, and is there likely a reaction from them? Sharing or liking a site that goes against some position taken by the government, may drag one into unnecessary trouble and may even lead to unnecessary prosecution [3, 26].

5. Assurance Considerations

An enterprise cannot have overall control over the use of mobile devices. Yet, they need to be managed, controlled, and secured by enterprise-wide policies, standards, and procedures, allowing audit professionals to verify that controls and safeguards stated in the policies are implemented to prevent data leakage or loss. Employees need to be aware of the sensitivity of information available to them. Or perhaps, they may be unaware of other vested interests creeping into their information, or they may not notice people shoulder surfing while they are at work [24]. Fig. 3 shows some statistics about people involved in “digital government” according to the incidents reported to SLCERT/CC [14]. There have been shocking details of password management with regard to youth in the country.

Technical controls have a role to play in mitigating unauthorized disclosures. Furthermore, technical controls will not provide sufficient protection in situations where attackers deliberately try to gain access to information directly from employees. Staff need to be made aware in order to resist active attempts to collect sensitive or confidential information through psychological manipulation, i.e., social engineering attacks. Besides, there are various other ploys and tactics used by attackers to collect information from reluctant employees by using “impersonation, ingratiation, conformity, diffusion of responsibility, and plain old friendliness” [25]. However, technical or physical controls alone may not be the answer. An attitudinal change has to be cultivated in employees so they can be trusted to do the right thing if the business is to operate effectively.

Awareness that an enterprise has a sound mobile device strategy—including asset management, policies, technical controls, and awareness training—helps the enterprise to be in the know regarding the types of devices and traffic that are crossing the network, as well as how those devices are used. Frameworks such as COBIT and Risk IT [21] can provide a strong foundation for technology management.

Individuals need to rethink and check online habits regularly. Privacy set to the highest level can make it harder for attackers. Refuse third-party apps and services, and keep away from ads. They may be the means by which cybercriminals get into the network. Install a reliable security solution on computers and mobile devices. A privacy scanner can monitor social media accounts for weak privacy settings on Facebook, LinkedIn, Google+, and Twitter, and identify risky settings on different browsers.

6. Conclusion

Social media used for commercial purposes, thus cybercriminals may use the platform to draw users into participation in bogus causes, contests, and other promotional activities. Users of these social networking sites; may not be aware of how secure their posts online. There may also be privacy concerns due to complex impression management, and peer pressure to release more information. This could affect work performance and could cause higher level of vulnerability over time. Therefore, it is necessary for more holistic and longitudinal studies in order to understand them better.

Install only trust-worthy products as much as possible; always limit what these apps can access, and install an antivirus/anti-malware product. Secure screens with a lock; set up Find My Phone, activate Remote Wipe, and always remember: public networks are public. These suggestions could be a few of the means to ensuring data privacy and security.

References

[1] Yang Wang and Alfred Kobsa, "Privacy in Online Social Networking at Workplace", IEEE Int'l Conference on Computational Science and Engineering, Vancouver, Canada, pp. 975-978. Article (CrossRef Link)

[2] Vicen¸c Torra, Guillermo Navarro-Arribas "Big Data Privacy and Anonymization", Article (CrossRef Link)

[3] S.M. Buddika Harshanath "Privacy & Security in Mobile Devices, Social Network Services and Social Reform" International Conference on Inventive Communication and Computational Technologies (ICICCT 2018) Coimbatore, India. 2018. Article (CrossRef Link)

[4] Communication Services - Economic and Social Infrastructure of Annual Report 2016 of Central Bank of Sri Lanka. Page 94. Article (CrossRef Link)

[5] Digital in 2017: Southern Asia Article (CrossRef Link)

[6] Airline websites don't care about your privacy: a case study on Emirates.com Article (CrossRef Link)

[7] Information We Automatically Collect from You ISACA Privacy Notice Updated:1 May 2018 Article (CrossRef Link)

[8] "Securing Mobile Devices" Article (CrossRef Link)

[9] "Are texting and Facebook worse for teens than TV?" Article (CrossRef Link)

[10] S.M. Buddika Harshanath "Privacy & Security in Mobile Devices, Social Network Services as Related to Business" International Conference on Intelligent Computing and Control Systems (ICICCS 2018), Madurai, India, 2018. Page 1406-1411.

[11] "Big Data" Article (CrossRef Link)

[12] E. Bertino, Big Data – Opportunities and Challenges, Panel Position Paper, Proceedings of COMPSAC 2013. Article (CrossRef Link)

[13] "Data, data everywhere", The Economist, 25 February 2010 Article (CrossRef Link)

[14] "Information and Cyber Security Strategy of Sri Lanka" CERT report on 17th April 2018 by Sri Lanka Computer Emergency Readiness Team | Coordination Center Article (CrossRef Link)

[15] "Virtual private network" Article (CrossRef Link)

[16] "Sri Lanka lifts ban on Facebook imposed after spasm of communal violence" World News-Reuters; March 16, 2018 by Shihar Aneez, Ranga Sirilal Article (CrossRef Link)

[17] Paul Hoffman and Kornel Terplan, Intelligence Support Systems: Technologies for Lawful Intercepts (Auerbach Publications, 2006), Page 63.

[18] Beyond Privacy and Security The Role of the Telecommunications Industry in Electronic Surveillance by Mieke Eoyang By Mieke Eoyang, David Forscey Monday, April 11, 2016 Article (CrossRef Link)

[19] "Managing mobile devices and relevent framework procedure" Article (CrossRef Link)

[20] Amelia Heathman "The best Android security apps to keep your phone and tablet safe - Make sure all your data is secure with these mobile security apps" Article (CrossRef Link)

[21] "COBIT Framework for IT Governance and Control" Article (CrossRef Link)

[22] "Risk IT Framework for Management of IT Related Business Risks" Article (CrossRef Link)

[23] "Social Engineering Fundamentals, Part I: Hacker Tactics." Article (CrossRef Link)

[24] "APNewsBreak: University posts info of 40K students" Article (CrossRef Link)

[25] Tuhin Borgohain,Uday Kumar,Sugata Sanyal "Survey of Security and Privacy Issues of Internet of Things" Article (CrossRef Link)

[26] "Major Social Media Platforms-Social Media Marketing" Article (CrossRef Link)

S M Buddika Harshanath received his B.S. degree in from University College Dublin (UCD), Ireland, in 2004. In 2007, he earned M.S. degrees in the field of Information Technology from Sri Lanka Institute of Information Technology (SLIIT). Works at the department of Software Engineering, Faculty of Computing at the SLIIT. He was involved in supervising various undergraduate projects including Fashion Fit, Diet Master, Give Away, His research interests include Security and Privacy, Machine learning, Artificial Intelligence and Computer Vision.