Digital Fingerprint and Security Aspects in Internet of Things Against Social Engineering Using Advanced Digital Forensics

Rubika Walia[1], Neelam Oberoi[2], Ajay Kumar[3] Gulbir Singh[4*]

[1,4]Assistant Professor, MMICT&BM, M. M. (Deemed to be University), Mullana, Ambala, Haryana, India
[2]Assistant Professor, Department of Computer Science and Engineering, M. M Engineering College, M. M. (Deemed to be University), Mullana, Ambala, Haryana, India.
[4]Head of Department and Associate Professor, SRM Global, Naraingarh, Ambala, Haryana, India.
[1]ahluwalia.rubika@gmail.com, [2]neelamoberoi1030@gmail.com, [3]katiyarajay30@gmail.com,
[4*]gulbir.rkgit@gmail.com

Article Info
Volume 83
Page Number: 4914 - 4920
Publication Issue:
March - April 2020

Article History
***Article Received**: 24 July 2019*
***Revised**: 12 September 2019*
***Accepted**: 15 February 2020*
***Publication**: 27 March 2020*

Abstract

Now days, the dependency on the smartphones and the web applications are elevating to huge extent and thereby the need to work on the security and privacy is there. As per the Annual Reports from prominent platforms of antivirus and malware analytics patterns, the there are millions of attacks per month on the network based environment. With the implementation patterns of advanced tools and technologies including Python based packages and open source distributions, the overall performance can be elevated. The presented research manuscript is presenting the use cases and the implementation patterns for the cyber security in IoT based scenarios with the effectual cases and overall performance with the cumulative analytics. Python integrates more than 2 lac tools and libraries which can be used for scientific, mathematical, engineering and social applications with cyber analytics patterns. All these tools and frameworks can be integrated from the repository of Python software. As the research scholars, academicians and practitioners keep on working with research projects, the Python based tools can be used because of the ease as well as high performance programming.

Keywords; *Cyber Security, Digital Fingerprinting, Digital Security, Social Engineering, IoT.*

I. INTRODUCTION

Internet of Things (IoT) is now days in huge usage patterns whereby the need arise to work on the high performance scenarios [1, 2]. The news reports show are that there quite significant elevation in the outcomes and analytics [3, 4]. With the increasing dependency and huge usage of online platforms, the issues and concerns of security and privacy are getting attention. A number of cases associated with data breach, hacking, data leakages, server cracking and many others are reported everyday in the global news which creates panic towards the use of online platforms whether via web applications or smartphone apps. There is need to propagate the awareness with the use of online platforms so that multi-dimensional security and privacy can be maintained.

To cope up with the hacking and data breach attempts, there is need to secure the web and smartphone applications against malicious attempts. A number of tools and frameworks are available which are widely used for the penetration testing and digital forensics. These tools are suggested to be used by the application developers so that the information leakage from the software cannot be successful.

II. REVIEW OF LITERATURE

With the gigantic usage of astute contraptions and advancement based stages for individual similarly as real correspondence, the data is getting extended in various plans. These data records and envelopes are required to be taken care of for at some point later anyway security is the huge concern so the set away data can be recuperated with least exchange speed and high checked way. The consistent data extraction and assessment is one of the key spaces in orchestrated applications including incline data examination, criminal data assessment, advanced watching, sentiments mining, factual looking over and various others (Somayya Madakam, R. Ramaswamy, Siddharth Tripathi (2015)). This system is generally called web scratching and comprehensively used in the farsighted mining and data disclosure constantly with the objective that the certified data about the specific individual or article can be seen from web based life. Similar sort of utilization is done by the ideological gatherings to get the inhabitant overviews about their social affair with the probabilities to win in the choices. In addition, such procedures are in like manner used by the corporate goliaths to get the analysis about their thing from generally populace.

The key features with the support and recovery stages fuse the going with perspectives

- Support for various stages and mobile phones
- Support for PDA applications
- Minimum move speed
- Enormous record bunches for moving
- Cloud applications for adjusting the records on-the-fly
- Minimum resource usage
- Portability with assembled working structures

Security against unapproved access with conspicuous evidence of getting to devices.

In the current days, the data is being transmitted in gigantic associations for corporate and singular use including web based life, online business doors, visit applications, social occasions and various others. For routine applications, it is imperative to store the data for future usage so that at whatever point wherever availability of data will be there.

III. KEY SCOPE AND DIMENSIONS

The figures used in the research reports are frightening and must be taken care by the forensic investigation agencies and law enforcement bodies. The cyber investigating teams and the government officials are required to be equipped with the advanced tools and programming languages so that any malicious attempt can be identified with the root cause of the crime [5, 6, 7].

Many computer code libraries, frameworks, tools and programming languages square measure already accessible for digital forensics and cyber security, during which each subject ought to bear in mind of. With the notice of those tools and technologies, the cyber attacks on privacy are unbroken safe [8, 9, 10].

Key Domains of Tools for Cyber Security and Digital Forensics

- Steganography
- Image Forensics
- Web Scraping
- Hidden Information Extraction
- E-mail Fingerprinting
- Remote Access Denial
- Video Forensics
- Vulnerability Analytics
- Internet of Things (IoT) Security
- Web Applications Security

- Anti-Exploitation Tools
- Anti-Sniffing and Anti-Spoofing Attacks

IV. METHODOLOGY

Many programming languages and tools already out there for cyber security and digital rhetorical applications however Python programming is sort of distinguished and wide used [4]. Python has lacs of modules on its official repository of PyPi.org of varied domains together with cyber security, grid computing, info security, cloud applications, internet scraping, image forensics and plenty of others. Python is one amongst the unremarkably used programming languages by the cyber security professionals as Python has huge tools and packages in free and open supply distribution [5, 11]. In addition to the determination and coordination of front line devices on web condition, there is need to ensure the security and reliability to the Internet related establishment. These can be confirmed using Blockchain Technology, Quantum Cryptography, Multi-Factor Authentication and many checked systems which are critical for real applications. There is need to work on the moved methodologies for the security careful segments due to which the complete security can be raised. The investigation unique duplicate is showing Python gadgets and structures for the pushed executions towards security and dependability. Python is the key development and programming structure that is commonly planned for the legitimate applications and advanced security mix towards massive spaces for the all out execution and tremendous tallness in the reasonability. The displayed work is entirely practical in the immense points which are used for the policing similarly as shield establishments whereby the colossal consolidations are required for the huge executions on the security viewpoints and massive statures in the observable viable perspectives. The work and the procedures can be used for the national obstruction and the computerized security models and the utilization to achieve the more raised degrees of genuineness and execution in the general circumstances for the huge applications. Every digital image is having the Exchange Information (EXIF) data which will be wont to determine the particular camera or device victimization that that image is taken. Python provides several libraries and packages for EXIF information to acknowledge the basis of a microorganism image. Python integrates the package Python Image Library (PIL) for image analytics and rhetorical applications. it's additionally used for the extraction of EXIF information to acknowledge the camera data furthermore because the location from wherever the image is taken. PIL package is out there because the redo as Pillow [7]. the combination is sort of vital and preponderating to possess the upper degree of performance and therefore the effectiveness.

V. ANALYSIS AND RESULT

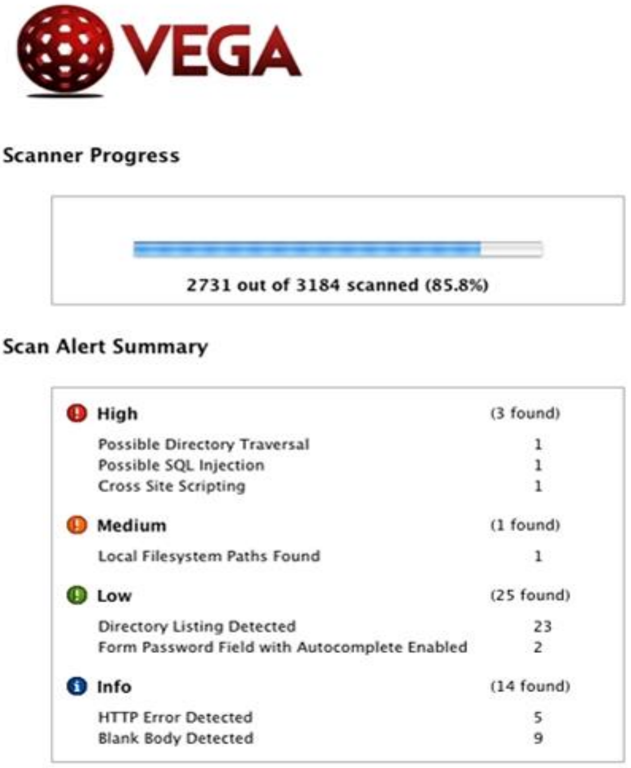
Security and Digital Forensics Mechanisms

Vega

https://subgraph.com/vega/

Vega is one of the powerful tools under free and open source distribution for penetration testing. It is used as web security scanned and effective platform for Cross Site Scripting (XSS) implementations. In addition, the test associated with SQL Injection and information disclosure can be evaluated. Vega Tool is GUI based tool written in Java and is cross platform.

Vega is developed and launched by Subgraph and available for cyber forensic and web penetration analytics.



Scanner Progress

2731 out of 3184 scanned (85.8%)

Scan Alert Summary

High	(3 found)
Possible Directory Traversal	1
Possible SQL Injection	1
Cross Site Scripting	1
Medium	(1 found)
Local Filesystem Paths Found	1
Low	(25 found)
Directory Listing Detected	23
Form Password Field with Autocomplete Enabled	2
Info	(14 found)
HTTP Error Detected	5
Blank Body Detected	9

Figure 1: Deep Analysis in Vega Scanner

The scanner progress in Vega tool presents the types of vulnerabilities with the associated impact in terms of High, Medium or Low. This type of outcome predicts the performance of web application and possible security breach points.

Penetration Testing and Audit of Android Based Smartphone Apps

In the current era, most of the web services and applications are deployed on smartphone platforms including Android, iPhone, Blackberry, KaiOS, Symbian, Java and many others. The software applications launched for mobile platforms are required to be tested rigorously against assorted assaults and vulnerability points.

Tool	URL
AAPT	https://androidaapt.com/
OWASP Zed Attack Proxy	https://www.owasp.org
QARK (Quick Android Review Kit)	https://github.com/linkedin/qark
Devknox	https://devknox.io/
Drozer	https://labs.mwrinfosecurity.com/tools/drozer
MobSF (Mobile Security Framework)	https://github.com/MobSF/Mobile-Security-Framework-MobSF
Mitmproxy	https://mitmproxy.org/
iMAS	https://github.com/project-imas/about

Android Asset Packaging Tool (AAPT) Tool

URL: https://androidaapt.com

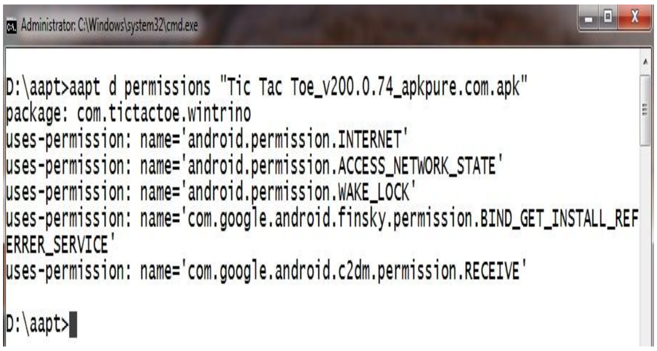
Now days, most of the smartphone apps are available on Android Operating System and widely used by the mobile phone users because of its prominence and availability in open source distribution. At the time of installing the Android App in Android Package (APK) format, it requires specific permissions which are generally ignored by the Android users.

With the increasing number of smartphones and mobile applications, there is need to check the vulnerabilities with these devices so that the misuse and exploitation cannot be done.

A number of cloud repositories are available from where the Android APK files are downloaded by the users including the following:

- https://apkpure.com/
- https://www.apkmirror.com/
- https://www.androiddrawer.com/
- https://apk-dl.com/
- https://en.aptoide.com/
- https://androidapksfree.com/
- https://www.appsapk.com/
- https://apk4all.com/

○ and many others



```
D:\aapt>aapt d permissions "Tic Tac Toe_v200.0.74_apkpure.com.apk"
package: com.tictactoe.wintrino
uses-permission: name='android.permission.INTERNET'
uses-permission: name='android.permission.ACCESS_NETWORK_STATE'
uses-permission: name='android.permission.WAKE_LOCK'
uses-permission: name='com.google.android.finsky.permission.BIND_GET_INSTALL_REF
ERRER_SERVICE'
uses-permission: name='com.google.android.c2dm.permission.RECEIVE'

D:\aapt>
```

Figure 2: Fetching APK Permissions using AAPT

Using AAPT tool, the permissions associated with the APK can be analyzed cavernously so that the attempts of data breach and unknown copying of information can be avoided. In some cases, the smartphone users do not download the Android App from Google Play Store and they directly download the APK from different other portals but it is quite dangerous and advised to analyze the inherent permissions using advanced tools before installing on the mobile phone.

In addition, the research scholars and practitioners can work on this domain of smartphone malware analysis by collecting the permissions from assorted APK files and then training the datasets using machine learning. By this approach, the predictions on upcoming smartphone apps can be done in terms of their security, privacy and data breach issues.

Web Server Fingerprinting

The Web Server Fingerprinting can be done effectively in the scenarios to have the cavernous analytics.

>>> import socket

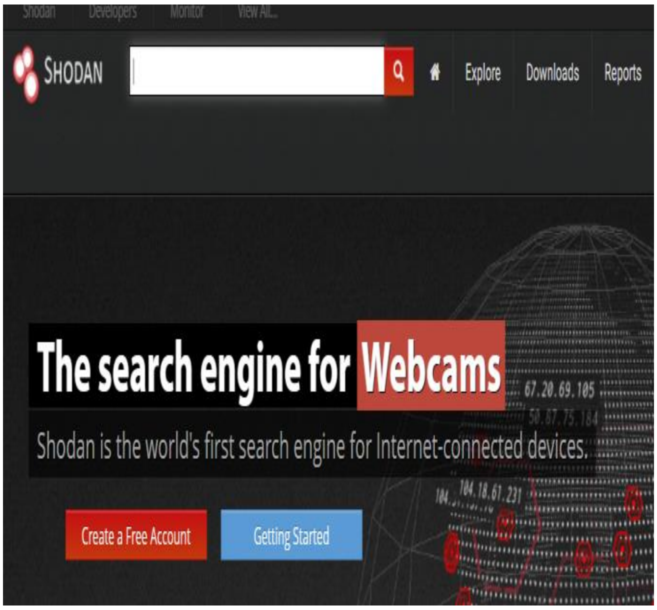
>>> socket.gethostbyname(‘URL')

>>> socket.gethostbyaddr(‘IP Address')

Using these in-built functions of Python, the URL or IP address can be tracked. In addition, there are assorted libraries in Python which are used for the extraction of deep information about the devices or remote systems.

Security Aspects of CCTVs and Webcams

In this era, there square measure huge sensible gadgets and webcams that square measure connected on IoT network atmosphere with the informatics addresses. These informatics primarily based webcams square measure indexed by the specialised search engines and Shodan is one among them. Shodan (shodan.io) is one among the notable search engines that indexes and saves the data of informatics primarily based webcams. By merely putting in the webcams, the safety and integrity can not be enforced till the safety of the informatics addresses isn't ensured. Shodan is ready to fetch the data concerning webcams and IoT devices that square measure vulnerable.



The search engine for Webcams

Shodan is the world's first search engine for Internet-connected devices.

Figure 3: Shodan Search Engine for Webcams and IoT Devices

On creation of account on Shodan, the API secret's generated from uniform resource locator https://account.shodan.io and it are often used for the procedure and deep data concerning the IoT primarily based devices.

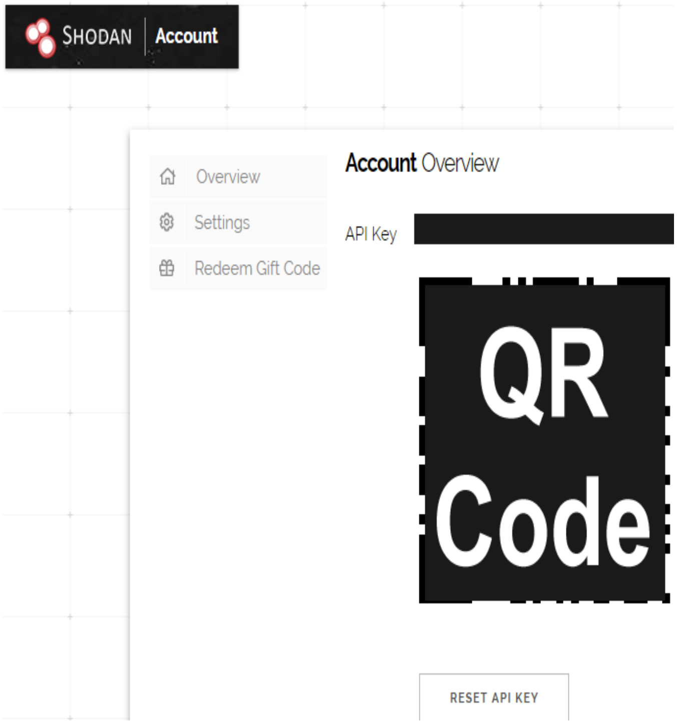


Figure 4: API Key and QR Code by Shodan

The Shodan based library is available in Python so that the analytics of data and its results can be fetched with the higher degree of performance.

```
import shodan

SHODAN_API_KEY = "***************************"

shodanapi = shodan.Shodan(SHODAN_API_KEY)

thishost = shodanapi.host('Target IP Address')

print("""

    Extracted IP: {}

    Extracted Organization: {}

    Extracted Operating System: {}

""".myformat(mymyhost['ip_str'], myhost.get('org', 'n/a'), mymyhost.get('os', 'n/a')))

for item in mymyhost['mydata']:

    print("""

        Extracted Port: {}

        Extracted Banner: {}

    """.format(item['port'], item[my'data']))
```

To ensure the security and privacy of the webcams and IoT gadgets, the integration of advanced strong passwords should be done. If strong passwords to webcams are not given, then anybody can access the remote webcams using Python scripts.

VI. CONCLUSION

IoT integrated cyber security and forensic analytics is one of the key sectors in the globally in multiple domains including Medical Science, Information Technology, Bio-Informatics, Agriculture, Banking, Finance, Stock Market, Space Science, Cyber Security, E-Commerce, Gaming, E-Governance and many others. The global market for Cyber Scientists is getting hot and there is bulk requirement in the corporate as well as government sector to deal with and analyze the data for predictive analytics and knowledge discovery. Now days, the organizations are hiring the professionals having practical exposures in data science, machine learning, artificial intelligence and big data analytics. Python Programming Language is getting huge fame because of the abundance of tools and packages in less number of lines of code. In traditional programming languages, the algorithms are required to be implemented from scratch but Python is having the packages in which the algorithms and techniques are programmed and deployed for the researchers and cyber analytics based data scientists.

REFERENCES

[1] Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tutor. 17 (2015) 2347–2376.

[2] C. Perera, A. Zaslavsky, P. Christen, D. Georgakopoulos, Context aware computing for the internet of things: A survey, IEEE Commun. Surv. Tutor. 16 (2014) 414–454.

[3] H. HaddadPajouh, A. Dehghantanha, R. Khayami, K.-K.R. Choo, A deep recurrent neural network based approach for internet of

things malware threat hunting, Future Gener. Comput. Syst. 85 (2018) 88–96.

[4] Kumar, G., Singh, G., Bhatanagar, V., & Jyoti, K. (2019). Scary dark side of artificial intelligence: a perilous contrivance to mankind. *Humanities & Social Sciences Reviews*, *7*(5), 1097-1103. https://doi.org/10.18510/hssr.2019.75146

[5] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Comput. Netw. 54 (2010) 2787–2805.

[6] M.A. Khan, K. Salah, Iot security: Review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. 82 (2018) 395–411.

[7] Nieto, R. Rios, J. Lopez, Iot-forensics meets privacy: towards cooperative digital investigations, Sensors 18 (2018) 492.

[8] R. Hegarty, D. Lamb, A. Attwood, Digital evidence challenges in the internet of things, in: Proceedings of the Tenth International Network Conference, INC, Lulu. com, 2014, p. 163.

[9] Alabdulsalam, S, K. Schaefer, T. Kechadi, N.-A. Le-Khac, Internet of things forensics: Challenges and case study, 2018. ArXiv preprint arXiv:1801.10391.

[10] Singh, G., Kumar, G., Bhatnagar, V., Srivastava, A., & Jyoti, K. (2019). Pollution management through internet of things: a substantial solution for society. Humanities & Social Sciences Reviews, 7(5), 1231-1237. https://doi.org/10.18510/hssr.2019.75162

[11] Hoon Kim, T, C. Ramos, S. Mohammed, Smart city and iot, Future Gener. Comput. Syst. 76 (2017) 159–162.