A Study on IoT security: Threats, available solution architectures, challenges of current solutions, and further possibilities.

Kartikey Raj Tiwari(IEC2017080), Raghav Dhupar(IIT2017121)
Navneet Kumar(IEC2017053), Naga Venkata Sriram Gadde(IIT2017126)
Amit Raj (IIM2017008)

***Abstract*— The Internet of Things (IoT) is the next generation of communication. Using the IoT, substantial objects may be authorized to generate, collect, and trade records in an unbroken manner. Various IoT applications aim on automating exceptional tasks and are trying to empower the inanimate physical items to act with no human intervention. The existing and upcoming IoT applications are fairly promising to growth of the degree of comfort, efficiency, and automation for the users. To be capable of implementing this type of world in an ever-growing fashion requires an excessive security, privacy, authentication, and recovery from attacks. In this regard, it is imperative to make the specified changes in the architecture of the IoT packages for achieving end-to-end secure IoT environments. In this paper, a detailed overview of the safety-associated demanding situations and sources of threat within the IoT packages is presented. After discussing the safety issues, numerous emerging and current technologies centered on accomplishing a high level of trust inside the IoT applications. We have discussed three exceptional technologies, blockchain, fog computing, and Machine learning, to increase the extent of safety in IoT. Moreover, based on analysis, challenges and further possible solutions have been discussed.**

Keywords: *IoT- Internet of Things, IoT security- Internet of Things security, IoT applications- Internet of Things applications.*

I. INTRODUCTION

WITH the rapid evolution of information and communication technologies, mobile Internet, and The Internet of Things (IoT) have become indispensable in daily life. The Internet of Things (IoT) is the next period of communication. Utilizing the IoT, physical objects can be engaged to make, get, and trade information in a consistent way. Different IoT implementation center around robotizing various undertakings and are attempting to enable the lifeless physical items to act with no human intervention. The existing and upcoming IoT applications are exceptionally promising to boom the level of comfort, efficiency, and automation for the users.

Apart from non-public use, IoT serves the community wishes as well. Various smart devices that perform diverse functionalities including monitoring of surgical procedure in hospitals, identifying weather conditions, providing tracking and connectivity in automobiles, and identity of animals the usage of biochips are already serving the community-particular wishes. As the foundation of those networks, the mobile community has been designed to aid Internet connectivity and to complete the internetworking of all the devices. This fact, therefore, leads to complicated community architectures, community topologies, get entry to technologies, service requirements, and mobile equipment even as bringing critical security issues in wireless information transmission.

How to guarantee the safety of confidential information has end up the precondition to the commercial application of a few emerging wi-fi networks and communique services. Therefore, the theories and technology of data security have attracted increasing worries from each academia and enterprise recently.

The Internet of Things is poised to become a part of ordinary life for maximum people.

There has been a great effort in recent years to cope with safety issues inside the IoT paradigm. Some of these processes target protection problems at a specific layer, whereas, other methods purpose at providing stop-to-stop safety for IoT.

II. SOURCES OF SECURITY THREATS IN IoT APPLICATIONS

A detailed interpretation to both the approaches will be given in this section. We can divide the IoT application into four main layers: (1) perception layer; (2) network-layer; (3) service layer; and (4) application layer. Each of these layers in an IoT application uses diverse technologies that bring several issues and security threats.

1-PERCEPTION LAYER: Insufficient security configurability is due to the hard-coded credentials which are often used within IoT devices. Hard-coded credentials are easy to compromise due to the use of the same password by many devices. Poor physical security is another attack vector caused by a vulnerability in the hardware. The main obstacle in encrypting the devices is due to the simplicity of devices such as sensors. Furthermore, there might be a conflict in terms of the usability of the product. Mentioning below the different types of attacks that might be possible:-

1-Booting Attacks During the booting process, the edge devices are at risk of being attacked by several attacks because of the disabled security process at that instant. Taking advantage of this situation, the attackers may try to attack the node devices when they are being restarted.

2-Wrong data injectionOnce a node becomes captured, the attacker can easily use it to inject erroneous data onto the IoT

system. This may lead to false results and IoT Application might start malfunctioning.

3-Node Compromise IoT applications comprise of several low power nodes such as sensors and receptors. These nodes are vulnerable to a large number of attacks. The attackers may try to capture or replace the node in the IoT system with a malicious node. Now the new malicious node is operated by the attacker but it seems to be the part of the system.[1]

4-Malicious Code Injection In this attack the attacker injects some malicious code in the memory of the node. Generally, the software of IoT nodes are upgraded in real time on the air, and this gives an opportunity to the attackers to inject malicious code into device's memory.

5-Side-Channel Attacks The micro-architectures of processors, electromagnetic emanation, and their power consumption reveal sensitive information to attackers. Side-channel attacks can be based upon abnormal power consumption, laser-based attacks, timing attacks ,or electromagnetic attacks.

6-Sleep Deprivation In these types of attacks the attackers try to drain the battery of the low-powered IoT physical layer devices. This eventually leads to a denial of service from the nodes(i.e.,DDoS) in the IoT application due to a dead battery.

2-NETWORK LAYER The main function of this layer is to send the data received from the perception layer to the computational unit for processing. At this layer, several security threats are encountered, which are discussed below:-

1-Phishing The attacks in which several IoT devices are targeted by a minimal effort put by the attacker are referred to as phishing attacks. There is a possibility of encountering phishing sites during the time when users visit web pages on the Internet. Once the user's account and password are revealed somehow, the whole IoT environment of which user is a part of, becomes vulnerable to cyber-attacks.[22]

2-Advanced persistent threat(APT) When the IoT network can be accessed by an unauthorized person or an attacker, then this type of attack falls under APT. The attacker may continue to stay in the network undetected for a long period of time. The main intention of this attack is to steal some valuable information instead of damaging the network or its resources.[3]

3-Denial of Service Attacks Attackers can easily launch DDoS attacks on the IoT servers because many IoT devices in IoT applications are not strongly configured and thus may easily serve as gateways for the adversaries. The attackers flood the target servers with a large number of unwanted requests. This immobilizes the target server, further obstructing the services to the genuine users. Due to the heterogeneity and complexity of IoT networks, the network layer of the IoT is prone to such attacks.[4]

4-Data Breaches The hackers and other adversaries always target the valuable information of the users. In IoT applications, there is a large volume of data moving between sensors, actuators, cloud, etc. Different connection technologies are used in such data communications, and hence the IoT applications are vulnerable to data breaches.

5-Routing Attacks During the data transmission, the routing paths are tried to being redirected by the malicious nodes in an IoT application. (e.g.,Sinkhole Attacks & Wormhole attacks)

3-SERVICE LAYER The main purpose if the service layer in the IoT applications is to make a middleware abstract layer between the network layer and the application layer. It may also provide powerful computing and storage capabilities[5]. This layer provides APIs to meet the needs of the application layer. The service layer contains brokers, persistent data stores, queuing systems,ML etc. It is also susceptible to various attacks. These attacks can potentially take control over the entire IoT application by infecting the service layer in worst case.

1-Man in middle attack The MQTT protocol uses publish-subscribe model of communication between clients and servers using the MQTT broker, which effectively acts as a proxy. It enables the decoupling of the publishing and subscribing clients from each other and messages can be sent without the knowledge of the destination.

2-SQL injection In such attacks, The attacker can embed malicious SQL statements in a program[6],[7]. Then the invaders may get access to the private data of any user and can change records in the database [8]. SQLi has been listed as top security threat to web by Open Web Application Security Project in their OWASP top 10 2018 document[9].

3-Flooding Attack These types of attacks pose a huge impact on cloud systems by augmenting the load on the cloud servers. This functionality of this attack is very similar to that of DoS attack in the cloud and mostly quality of service is affected by this attack.The attackers continuously send large number of requests to a service,in order to deplete resources in the cloud.

4-Cloud Malware Injection In these kinds of attacks, the invaders can get control, inject malicious code, or can injection a virtual machine into the cloud.

4-APPLICATION LAYER THREATS This layer is mainly comprised of the IoT applications like smart homes, smart meters, smart cities, smart grids, etc. This layer is at a high risk to some particular security issues that aren't found in other layers, such as information theft and privacy threats. The security problems in this layer are also specific to exceptional applications. Main security troubles encountered with the aid of the this layer are mentioned as follows:

1-DDoS Attacks There have been various instances of such attacks on IoT applications. Such attacks prevent genuine users from using the services of IoT applications by intentionally making the servers busy in processing other spam/unwanted requests.

2-Malicious Code injection If a system doesn't have sufficient code checks it makes the system vulnerable to malicious scripts and misdirections and in such case the attacker may use makicious code injection as an entry point to the IoT environment. Normally, XSS(cross-site scripting) is used by

the invaders to inject some malicious script into an otherwise trusted website.

3-Data Thefts There is a lot of data movement that takes place in IoT applications and we know that the operational data is at a high chance to strike than static data. And if these applications are at risk to data theft attacks then the users will not register their private data on IoT applications.

4-Reprogram Attacks If the programming procedure is not secured, the invaders can try to reprogram the IoT objects remotely. This may lead to the hijacking of the IoT network[10].

5-Access Control Attacks This is an authorization mechanism that permits only authorized users or processes to access the data or account. Once the get admission to is compromised then the entire IoT application will become vulnerable to several styles of assaults it really is why get right of entry to manipulate assault is a totally severe attack in IoT applications.

III. SOLUTIONS TO SECURE IoT ENVIRONMENTS/APPLICATIONS

There are various strategies and methods to secure IoT environments and applications. These solutions may be divided into three fundamental categories: (1) Blockchain-based solutions; (2) FOG computing-based solutions; (3) ML-based solutions.

1. **BLOCKCHAIN BASED SOLUTIONS:** Blockchain tech is viewed by industry and studies community as a disruptive technology that is supposed to play a primary position in securing IoT systems. This section describes how blockchain can be an important technology for providing security solutions to today's challenging IoT security issues.

a-Identity Management Ownership of a device changes during the lifetime of the device from the manufacturer, supplier, retailer, and consumer. The purchaser ownership of an IoT tool may be changed or cancelled, if the device gets resold, decommissioned, or compromised. Managing of attributes and relationships of an IoT tool is a big challenge. Blockchain has been used widely for providing straightforward, trustworthy and authorized identity registration, possession tracking, and tracking of products, goods, and assets. The approaches like TrustChain have been proposed to ensure trusted transactions with the use of blockchain while keeping the integrity of the transactions in a diverse environment. IoT devices are no exception.

b-Data Integrity and Security Data broadcasted via IoT gadgets linked to the blockchain network will continually be signed with the aid of the real sender that holds a unique public key and GUID, which ensures authenticated facts. And considering that the facts is saved in a non-centralized way in The blockchain it results in better information security.

c-Authentication, Authorization & Privacy Blockchain smart contracts can provide decentralized authentication guidelines and logic on the way to offer authentication to an IoT Device.Also, smart contracts can offer more effective authorization access control to connected IoT gadgets with very less complication as compared with standard authorization protocols like OpenID, Role-Based Access Management (RBAC), OAuth 2.0. These protocols are widely used in recent times for IoT tool authentication, authorization, and management. Moreover, information privacy may be also ensured by the usage of smart contracts which set the access rules, conditions, and time to permit user or group of users, machines to own, control, or have access to data at a device/cloud or in transit.

d-Secure Communications With blockchain, key control and distribution are eliminated, as every IoT device has its unique GUID and asymmetric key pair once it is installed and linked to the blockchain network. This will cause a great simplification of other protection protocols as that of DTLS, with no need to deal with and alternate PKI certificates at the handshake section in case of DTLS or TLS (or IKE in case of IPSec) to negotiate the cipher suite parameters for encryption and hashing and to establish the grasp and session keys. Hence, light-weight safety protocols that would fit the requirements for the computational and memory resources of IoT gadgets turn out to be more affordable.

2. **FOG COMPUTING BASED SOLUTIONS:** Fog computing ideally demonstrates the concept of a distributed network environment that connects two different environments and is closely linked with cloud computing and IoT. This new computing paradigm was initially and formally introduced by Cisco to extend the cloud network border of the enterprise network[11]. The architecture of a Fog environment has three layers - the IoT layer, the Fog layer, and the Cloud layer. The IoT data collects data through its sensing devices and sends it to the devices of the FOG layer. The FOG devices carry out the information and send the results(as well as data in some cases) to the cloud for storage and further processing.

a-Network Security As The fog nodes are placed at the border of a network. All the data which enters the system through the perception layer has to pass through these fog nodes before entering the system thus this layer identifies unusual activities and can deal with the attacks(e.g., Man in Middle attack) before the attacker enters the system. Thus it offers additional security via performing as an intermediate security layer among end devices and cloud. Also as the end devices have resource constraint the nearby fog node can provide support to the end devices by performing security functions.

b-Data security As the quantity of nodes in the IoT surroundings increases the information generated by using end devices is likewise large. Since there is resource limitation at end devices data is generally sent to nearby fog node, this node further processes the data and sends it to other fog nodes for further processing and storage. As end devices are most vulnerable to attacks, storing data at fog nodes may provide enough security by using lightweight encryption and decryption techniques.

3. **MACHINE LEARNING BASED SOLUTIONS:**

a-DDoS Atack ML algorithms such as Decision Tree which is used as a main classifier or collaborative classifier with other ML classifiers in security applications, such as intrusion detection. For e.g., a previous study proposes the use of a fog-based system call system to secure IoT devices[12]. The research used Decision Tree to analyze network traffic to detect suspicious traffic sources and as a result, detect DDoS behavior.

b-Spoofing Attacks from spoofers can be avoided by using Q-learning [13], Dyna-Q, Support Vector Machines (SVM)[14], Deep Neural Network (DNN) model [15], incremental aggregated gradient (IAG)[17], and distributed FrankWolfe (DFW)[16] techniques. These techniques not only increase the detection accuracy and classification accuracy but also help in reducing the average error rate and false alarm rate.

c-Digital Signature Digital signature is one of the very promising ways of building trust between the user and the IoT applications. Several ML-based algorithms are being used for matching fingerprint patterns with speed and accuracy (e.g., in SVM based methods a feature vector is built based upon the pixel values of the fingerprint and is used to train the SVM. Later this trained SVM is used to detect fingerprints by matching various patterns[18])

d-Eavesdropping Attackers can eavesdrop on messages during data transmission. To protect from such attacks, ML techniques such as Q-learning based offloading strategy[19] or non-parametric Bayesian techniques[20] can be used. We can also use schemes like Q-learning and Dyna Q and ML techniques to protect devices from eavesdropping.

IV. DISCUSSIONS AND ANALYSIS

This section talks about the current challenges of various proposed techniques for ensuring IoT security and suggests methods to improve the current scenario of IoT security

1. **BLOCKCHAIN:** As we know blockchain was not developed for IoT environments thus in classical blockchain nodes cannot find each other over a network. e.g., Bitcoin Applications where bitcoin client is embedded with IP addresses of the senders which helps nodes to build the network topology. But since IoT devices are mobile, this approach won't work for IoT environment's changing topology.

Moreover, as we know IoT environments have a continuous increase in several nodes. The present blockchain technology scales poorly with an increase in the number of nodes. This can lead to centralization which would be a big drawback of Blockchain in IoT security.

One of the main characteristics of blockchain is it minimizes (sometimes may eliminate) the need for the backserver for storage of data and nodes IDs ,although ledger is saved in nodes. with increase in number of nodes, there is also an increase in the size of the ledger. And as we know the end devices in IoT have very limited resources it becomes a major issue to be solved shortly.

The heterogeneous nature of IoT environments is a challenge for blockchain-based security and storage methods. As IoT consists of a large number of devices with different resources and computational abilities. Not all of them will be able to run encryption or decryption within the same time or resource constraints. Thus blockchain must be dynamic to be implemented to an IoT environment.

Smart Contracts- These are scripts saved on the blockchain. The main advantage of these smart contracts is their flexible nature. along with encryption and storage of data it also restrict the access to data linked or desirable end devices and with the programmable ability for utilization of data with inside self -executing workflow of logical operation among end devices . . Using Smart Contracts would improve data security and integrity in IoT moreover it may improve operational efficiency.

Security- Use of blockchain might increase security in IoT environments but we need to address the question that what should be the optimum platform for integrating IoT with blockchain. Further, there must be laws from the local administration regarding the use of Blockchain technology. As this technology is new it doesn't have any legal compliance till now which makes it vulnerable.

The consensus mechanism that depends on the miner's hashing ability can be compromised ,hence permitting hackers as a host for blockchain technology . hence same way private security keys with predictability can be used for unusual attacks for security accounts .hence concluded that there should be a well defined mechanism for assurance of transactions and avoidance of race attacks which may result in double spending while transacting .

2. **FOG COMPUTING:** FOG layer provides the facility of Transient Storage which enables users to store data temporarily at the nodes. It has several benefits but it comes with security challenges. As we know the end devices are most vulnerable the same data that is recorded by the end device may be sensitive for one user and not very sensitive for another user, this may be related to health information, social events, etc. Thus it becomes important for identifying and securing sensitive data from a large volume of information.

Since the data is usually secured with encryption, No one other than the owner can decrypt it, this leads to a problem in data sharing to avoid these cryptography techniques like proxy re-encryption, attribute sharing must be implemented in FOG layer. Intrusion detection algorithms need to be implemented at the FOG layer for detecting malicious activities or policy violations. This is because the attacks normally target local services rather than whole architecture and the security of local services and resources can be ensured by making fog nodes collaborate with other nodes to ensure a proper intrusion detection algorithm.

Fog nodes may need to accumulate data in certain cases to avoid communication overhead and data leakage. To ensure the security of data in such cases encryption schemes similar to BGN encryption[21] and Paillier encryption[2

can be used for ***secure data aggregation***
As per the existing architecture when the FOG layer is unable to process a request it forwards it to the cloud for processing, We suggest inter fog resource sharing for processing requests on the FOG layer itself and avoiding unnecessary traffic to the cloud which would enhance security and speed of processing.
Moreover, we can implement various prediction and classification algorithms at the FOG layer to decide how long will a request reside in the FOG layer before getting transferred to the cloud for further storage. Moreover, we can try to classify requests to further decide to retain the request in the FOG layer or forward it to the cloud.

3. **MACHINE LEARNING:** The advancing of ML and DL algorithms made them easy in breaking cryptographic implementations such as can be used in break cryptographic systems using SVMs Machine learning and deep learning algorithms are not as secure as they may cause leakage of data ,as far scurity is concerned , ML and DL algorithms are vulnerable to dominant attacks DL algorithms themselves are vulnerable to potential attacks, hackers can have ability to design a system that recognize working of these deep learning algorithms for generation of attacks ,hence it can be very difficult to detect and defend.
As per Researchers have suggested various threats in these algorithms are vulnerable to many undefined threats which can result deficiency of performance with proper accuracy such as poisoning(attacker injects malicious samples), evasion(generating adversarial samples), impersonation(the attacker attempts to act as providing original data samples, to break the ML algorithm) and inversion attacks(exploits the application program interfaces) such hacktrials exploit the security of users.
Establishing a lightweight DL which is optimising the quantity of data, to achieve the desired performance the reduction of the time, energy, and memory required to construct a is a significant step towards the implementation of on-board security deep learning model will be a prominent step in executing the process of on-board security mechanism for IOT services , thus it has a large future scope.
Blockchain which delivers a decentralized database will play a prominent role in securing IoT based architecture.these algorithms will also provide great back support for blockchain technology hence will have a accurate way finalising decisions and improved assessment ,clarification of data,along with comprehending the information and in most prominent way the trending technology of blockchain can back support machine algorithms by coming up with wide database capability in a decentralized way .
The development of computing GPUs (mobile GPU) with the advancement of ML and DL algorithms for IoT security will have an efficient offloading strategy important for efficiency.
Having a real time strategy for avoiding the future attacks and providing perception and shielding is highly recommended for optimum safety procedure ,especially for wide ranging IoT structure. Finally, it may reduce the computational complexity.
In Future utilizing the intellect surveillance ability of machine learning related algorithms for betterment of safety design architecture policies will definitely persuade safety and security norms with support of mods of operation inside any particular entreaty or defined application.
Various ML and DL algorithms with minimized computations like regression, SVM, CNN, etc can be utilized at the physical layer to minimize unnecessary movement of data by predicting values of immediate future and comparing with previous value sent to the cloud.

CONCLUSION

We have introduced different security dangers at various layers of an IoT application. We have covered the threats related to the perception layer, network layer, service layer, and application layer. We have also analysed the existing and proposed solutions for future to IoT security threats which includes blockchain, fog computing, and ML. Different open research problems and issues that originate from the arrangement itself are also examined.
The state-of-the-art of IoT security has been discussed and analysed with some of the future research directions to further enhance the security of IoT. We have likewise explored the main challenges and tried to exhibit the motives as to why the security methods in the cloud platform cannot be employed directly in this Fog computing when it comes to auditing. In this study, we have introduced a taxonomy, by considering numerous security issues and protection according to the Fog environment, as well as briefly introduced and discussed these issues retrospectively. Besides, we also discussed how blockchain could help to provide solutions to some of the data security concerns in the Fog environment.
In this research paper ,we went through various surveys and reviews regarding IoT safety mechanism and other related issues ,we differentiated various issues based on high level ,intermediate level and low level . we also lead to conclusion related to various procedures of the literature for gripping IoT secure structure for full reliability at various defined levels .A guided analysis for IoT threats with their optimum solution has been discussed ,we also focus on various threats insinuation and their counterparts also been proposed .we emphasis hoe trending block-chain technology can be properly utilised and utilised as a required solution for various iot system threats . this research additionally traces and recognizes subsequent open research fields and summons

needed to be calibrate,in research field and suggested further possibilities to come up with authentic ,systematic adaptable IoT security heuristics .

REFERENCES

[1] S.Kumar, S. Sahoo, A. Mahapatra, A. K. Swain, and K.K.Mahapatra,"Security enhancements to system on chip devices for IoT perception layer," in Proc. IEEE Int. Symp. Nanoelectron. Inf. Syst. (iNIS),Dec. 2017, pp. 151–156.Jingrong Chen*, Lei Kou, Xiaochuan Cui.

[2] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Springer, 1999, pp. 223–238.

[3] Li and C. Chen, "A multi-stage control method application in the fight against phishing attacks," in Proc. 26th Comput. Secur. Acad. Commun. Across Country, 2011, p. 145.

[4] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT:Mirai and other Botnets," Computer, vol. 50, no. 7, pp. 80–84, 2017.4

[5] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "A survey of middleware for Internet of Things," in Recent Trends in Wireless and Mobile Networks. Springer, 2011, pp. 288–296.

[6] Q. Zhang and X. Wang, "SQL injections through back-end of RFID system," in Proc. Int. Symp. Comput. Netw. Multimedia Technol., Jan. 2009,

[7] R. Dorai and V. Kannan, "SQL injection-database attack revolution and prevention," J. Int. Commercial Law Technol., vol. 6, no. 4, p. 224, 2011

[8] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of Things: A survey," IEEE Internet Things J., vol. 3,no. 1, pp. 70–95, Feb. 2016.

[9] Acunetix. Insecure Deserialization. Accessed: Feb. 9, 2019. [Online].Available: https://www.acunetix.com/blog/articles/owasp-top-10-2017/

[10] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 3, pp. 355–373, 2018

[11] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM, 2012, pp.13–16.

[12] S. Alharbi, P. Rodriguez, R. Maharaja, P. Iyer, N. Subaschandrabose, and Z. Ye, "Secure the internet of things with challenge response authentication in fog computing," in Performance Computing and Communications Conference (IPCCC), 2017 IEEE 36th International, 2017, pp. 1-2:IEEE.

[13] L. Xiao, X. Wan, and Z. Han, "PHY-layer authentication with multiple landmarks with reduced overhead," IEEE Trans. Wireless Commun., vol. 17, no. 3, pp. 1676–1687, Mar. 2017.

[14] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?" IEEE Signal Process. Mag., vol. 35, no. 5, pp. 41–49, Sep. 2018.

[15] N. A. Alias and N. H. M. Radzi, "Fingerprint classification using support vector machine," in Proc. 5th ICT Int. Student Project Conf. (ICT-ISPC), May 2016, pp. 105–108.

[16] L. Xiao, C. Xie, T. Chen, H. Dai, and H. V. Poor, "A mobile offloading game against smart attacks," IEEE Access, vol. 4, pp. 2281–2291, 2016.

[17] L. Xiao, Q. Yan, W. Lou, G. Chen, and Y. T. Hou, "Proximity-based security techniques for mobile users in wireless networks," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 2089–2100, Dec. 2013

[18] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in Proc. Theory Cryptogr. Conf. Springer, 2005, pp. 325–341.

[19] APWG. Phishing Activity Trends Report. https://docs.apwg.org/reports/apwg$_t rends_r eport_q 4_2 017.pdf$