iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** XI **Month of publication:** November 2020

DOI: https://doi.org/10.22214/ijraset.2020.32216

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue XI Nov 2020- Available at www.ijraset.com

A Study on Efficient Battery Management System Providing Features to Resolve Damage occurring in Mobile Phones

Alakananda Giri
Academic Research Student, Department of Information Technology, B.K. Birla College of Arts, Science and Commerce (Autonomous) Kalyan, Thane, India

Abstract: ***One of the major concerns in this living mobile era is the thriving life span of our mobile phones. One of the most probable concerns is regarding leaving the mobile phones under charging especially during overnight to get sufficient charging time which in turn leads to overcharging and heating up. Although sometimes it may not be considered as a concern for some latest devices still we are looking for a perfect battery life for our inseparable buzzing friend. This paper provides a run through on some efficient ways to contribute to a perfect battery by browsing across certain criteria we tend to miss generally. The paper also showcases on a type of malicious attack which is performed on these devices when being charged i.e. battery exfiltration. It also contributes on the search for a battery backup using cloud computing to not only to avoid heating up of the device leading to damage but to also provide optimum utilization of charge. An overview on how an effective battery management system should be, on the latest mobile devices is the objective.***

Keywords: Battery, BMS, Virtualization, Storage, Cloud, Attacks, Exfiltration

I. INTRODUCTION

Battery is one of the most vital features be it in a mobile device, laptops, PCs or even in electrical vehicles. Whenever there is a need to buy a phone, it is one of the features which is checked along with other features: whether the battery is long lasting or not? Especially for a person who opts a mobile phone based on gaming purposes. The fast charging or the reverse charging are the features which add color to the rainbow. But is there a proper consideration for bringing light on the attacks, which are faced due to these convenient features provided in the devices? The answer may be initially why there is a need to care about that. True, but required phone must be long lasting is one of the desired features so there is a need to consider the crisis which may occur in the later stages too which indeed will be glanced in the further section. Also, there is a great chance of these attacks happening in the initial stages as well. The best thing to do is to find out a safe as well as efficient method to make batteries last longer, prevent attacks, protect it from damage, maintain its life in the long run and many other features. To provide the above-mentioned features, one must look at each problem which are faced in detail, analyze and find a solution to it. One vital thing to be considered is that when technologies maintain an ease to use characteristic there is a high chance, it is made prone to attacks as well. Since the demanding features include providing fastest and smartest methods which will not cause more time consumption and work efficiently, the things which are made easier for mankind, also allows an easy way for malicious attacks. Proper adaptations to prevent these is necessary, by preventing not curing after such cases occur. To attain the aim, consideration of the features which make BMS very efficient should be necessarily done one of them can be: an alarm system that induces sound or light a flash on the screen which are usual but other indications can also be introduced to make the alarm pleasant like introducing bubbles and spreading a fragrance. But for such indications, certain devices apart from mobile phones, laptops, pcs i.e. Internet of Things devices are required.

Cloud computing can be considered in order check whether we can establish a backup battery. The cloud is known for its flexible way for storage. Will it be the same for battery management system? This will be answered at the end of this study. The assumptions regarding this is that it could provide an efficient method for the same, if yes how will also be included. Since cloud can be used for storage of numerous kinds of data, there should be one such mechanism to store the battery remaining after the device is completely charged. Although not completely charged at least a certain amount must be present to use at battery-low conditions in case of emergencies. Security is always a concern let it be in any field not only in technology sector but all over the globe where data transfer and storage is concerned. The attacks through USB charging was already known, one of the harmful attacks. The newly found attack in recent time is through battery exfiltration.

Using the battery status API one can access the information of websites visited using such kinds of battery in a mobile device. Rather an interdiction attack, as it happens at workplaces by providing poisoned batteries. The problems related to such exfiltration will be analyzed. The last section will deal with a survey in which the participants will be asked to share their responses about having their ideologies about a desired BMS and with that certain criteria will be analyzed of how a change in the BMS system will be accepted by them and on what scores.

II. OBJECIVES OF THE STUDY

A. Reviewing on how cloud can be used as a medium to store battery and serve an efficiency in BMS
B. Discussing about the threats and scenarios occurring in batteries affecting BMS due to exfiltration
C. Analysis on population using mobile devices on a regular basis suffering various battery issues and their review on cloud as a platform for storage.

The above objectives would be completed on a margin of proving the specific hypothesizes through survey analysis, which are:
1) *H1:* "Cloud is a best alternative for having sensible battery backup in mobile phones in accordance to user convenience."
2) *H2:* "Data exfiltration is one of the majorly ignored threat affecting batteries in smart phones."

III. CLOUD AS A BATTERY STORAGE

Familiarity exists in searching for various efficient ways of storing battery by proper utilization of resources available. The solar, mechanical, wind may have succeeded to some level in establishing a space in BMS but still there is a need to have new advanced and safe ways and that's what a research looks forward to. There is an important need for it since battery is one of the major features in almost every sort of electronics. The digitalized era needs to make wireless communications possible in the developing devices to grow a major feasibility. Another important aspect is that the non-traditional ways of battery storage are reporting various major drawbacks like microwave energy when converted to electrical energy in form DC current results in a drawback of a large amount of heat conduction which is neither safe for devices nor for the users [21]. To overcome these, new ways of storage is undoubtedly needed. Cloud is overlooked as one of the vital ways of storing information. It provides a reduced cost and risk of having to maintain an IT environment instead providing resources required for the same. In short provides a significant direction in handling the economics in a wide section of areas. The highlight is that one no longer needs to be in front of any hardware components for any sort of networking or connection the cloud is the best alternative for every such scenario. One of the papers, cleared out a way through a technology which can make the hypothesis based on cloud storage for efficient BMS a truth [26].

A virtual battery is a tool which provides virtualization needed by the developers for various tasks. The virtualization is one of the major features of cloud through one can have a test environment embedded until a complete scenario is developed. A prototype produced for a project can be tested under surveillance of the features required for it and further checked for its working. Improvising is quite easy through this mechanism since actual development is completely virtualized. One of the advantages of this virtual battery which is brought into light is that it can store some battery power. Since the virtual battery tool is working on a virtual machine, the virtual battery enables a feature of discharging itself or in simple terms reduces its power and that power is saved and can be used as a battery for any device. The virtual battery mimics the battery discharge by utilization of a discharge thread [26]. The virtual battery already provides a mechanism of generating all battery related information including battery status information files based on the virtual machines using it. When the information related to low power conditions occur, the discharger acts accordingly and moves into a sleep state since there is a requirement needed. Since virtualization is a feature of cloud, this becomes quiet flexible. However, all of this depends on various factors like the discharge state and the amount of data or any kind of load the corresponding system. All these factors need to in a proper optimized state to store charge.

IV. BATTERY EXFITRATION AND RELATED ATTACKS

Data Exfiltration is one of the ignored types of attacks which needs to be considered on high risk. Speaking about batteries, the exfiltration exists, one may think of the usual mobile device related attack which affects battery, but it is not the case. The primary concern is when the device is purchased one never expects such a thing to happen and neither suspects at that time. The exfiltration of battery can occur by replacing the original batteries with poisoned ones. These batteries may act sound until sometime. The attacker may trace out these malicious batteries out with location and other sensitive data can be one scenario. There also may be a case that the charging process may turn out to be malicious by establishing a channel for some unknown wired or wireless connection to be a way of data leakage.

The hacking takes place through browsers which use Battery status APIs to know status and various other information of battery and this in turn lead to other attacks while acquiring information through browsers, cookies and even the access can exceed till the snapshots taken in the particular devices if connected to other apps. Another case of such an attack is that the hacker can embed malicious codes in a program which function for an unknown discharge or drain. Even the minimal sort i.e. getting a public gateway for hotspots or various authentication issues may occur due to these. One may only face the API attack when encountering such browsers which provide battery related information may in turn prove out to be even more dangerous. If such an activity keeps on happening, then an exfiltration channel will be formed through which accessing data and other sensitive information unethically will be convenient.

One of the major problems about exfiltration and an advantage at the same time for the hackers is that nobody would doubt about such an exfiltration happening in the devices since it may look like a battery drain attack like any kind of DoS or DoB attack and would never suspect from the place where the devices are bought or manufactured. Considering these attacks and providing proper counter measures to these will indeed help in development of an efficient BMS and prevent damage to mobile devices.

V. LITERATURE REVIEW

In a study published by Ferreira, D. et al. [1] in 2011**,** a large-scale study on battery life of android phones which included user's behaviour on charging and overcharging with solution suggested. The paper provided solutions to some of the battery issues the implementations of some of the solutions provided with proper experiments.

In a study published by D. J. J. M. T. N. [2] in 2017**,** A detailed study on the invention of an alarm in the smartphones with circuit design. The technology could give a rise to an efficient way to have BMS based on the concept that overcharging is one of the important factors affecting its long life.

In a study published by Ahmad, et al. [6] in 2017**,** It involved several battery-based frameworks, one regarding mobile phone another on cloud-based followed by a survey on Google Nexus Phone for battery estimation. The paper provided several frameworks for battery estimations it may be difficult to implement all of them in mobile devices. The conclusion was obvious regarding battery estimation for various mobile application.

In a study published by Harish N1, et al. [7] in 2018**,** The paper presented hydrogen emission by batteries and different battery parameters. Sending it to cloud in vehicles was another highlighting point. The paper discussed battery management systems focusing the topic regarding cloud which is appropriate to the current scenario.

In a study published by Sajedifar, et al. [10] in 2019**,** The following research paper provided information regarding the amount of dangerous electromagnetic emission from mobile phones by demonstrating a test on an HTC device. The paper demonstrated the adverse effects and the number of electromagnetic waves generated from a normal mobile phone

In a study published by Kim, et al. [11] in 2019**,** This paper presented a cloud related battery monitoring and management system along with fault prognosis and fault diagnosis detection and a variety of algorithms to resolve these. The paper provided a variety approach towards battery management through CMBP like newly designed algorithms for the same. Also, these methods were proven to be scalable, fast and cost effective which are the character tics which make a battery more efficient.

In a study published by Lifshits, et al. [12] in 2018**,** The paper experimented on the powerful and feasible malicious attacks due to overcharging of three popular mobile phones. The techniques used include data exfiltration directly from the server. Since paper provided the root causes of some of the new-bound attacks happening these days it provided a major impact on this part of research field.

In a study published by B. G. Schlicher, et al. [14] in 2016**,** The paper presented a successful technique to reduce data exfiltration by introducing a SDD approach which runs on FUSE.net. This approach minimizes a good amount of data leakage and thus helps to the motive of avoiding exfiltration. The technique introduced in this paper reduces data exfiltration but due to much of the protection provided to the data in this approach the accessibility and availability of data becomes difficult due to which this may be difficult to opt always.

In a study published by Albugmi, et al. [15] in 2016**,** The paper presented various data security threats found in cloud computing. Virtualization process having a risk due to hypervisor was also mentioned. Encryption security methods like cryptography were the methods which were brought to the focus. Although the paper made justice with its title it didn't provide sufficient of the same in the content. The methods for data protection in cloud computing was minimal. Major focus was more on cryptography security approach which is a traditional method of encryption. Other security threat detection methods and techniques could have also been mentioned apart from the traditional ones.

In a study published by Fiore, et al. [16] in 2017**,** The paper presented the battery drains cause and effects in mobile phones The paper included majorly on testing HTML 5 as a vector for battery drains and knowing its consequences when allowed it to be left unprotected from malicious attacks. The paper concluded by involving certain counter measures for the same.

In a study published by Ullah, et al. [17] in 2018**,** The paper reviewed upon a detailed study on exfiltration: one of the major concerns related to internet security. The paper examined 108 papers based on the following subjects and provided a detailed study on the countermeasures of data exfiltration. Particularly the paper also focused on the states of data exfiltration applicability on the basis countermeasure viz. 1. In use 2. In transit 3. At rest which provides an idea on which state of data particularly the attack takes place more and on what basis. The paper involved a detailed study on the exfiltration threats and its countermeasures. The states of availability of data exfiltration counter measures proved that more of the attacks were happening more on 'in use' state rather than 'in transit' and 'at rest'.

In a study published by Ioulianou, et al. [19] in 2019**,** The paper presented various Denial-of-Service Attacks based on Internet of Things devices. A platform named Cooja is one most attacked platform in case of IoT device was discussed clearly. An IDS was proposed in the paper for preventing the intrusions which require no firmware modification and prevents the vector from creating trafficking attacks wirelessly. The paper proposed a very new approach of providing an efficient IDS for malicious attacks however these are based on IoT devices only and are not confined to large scale system.

In a study published by Duh, et al. [20] in 2018**,** The paper demonstrated several High-Power Lithium-Ion Batteries used in various mobile brands like iPhone, Redmi, Samsung, Sony. Various factors including the temperature, thermal runaway, inflammable capacity etc was measured accordingly. The paper did well by comparing various devise based on the battery affecting factors, but the paper could have thrown more light towards the explanation of these factors and causes rather than the empirical part. Preventive measures could add more colour to create useful awareness.

In a study published by Jogendra Singh, et al. [21] in 2015**,** The paper presented a simple circuit along with a "Rectenna" which is a combination of antenna and rectifier. This rectenna will convert the microwave energy to DC current, hence producing electrical energy. A new form of wireless mobile charging through microwaves was introduced under this. The paper involved a new idea of using microwave signals to charge mobile phones which might indeed help in wireless charging in less amount of time and with reduced cost. Although the drawbacks related to heat generation and phone capability of handling "Rectenna" sounds a great issue. Modified version appropriate to overcome the above-mentioned drawbacks will lead to a better BMS.

In a study published by Hristozov, et al. [22] in 2019**,** The paper provided in an approach in the sense that the battery affecting factor is resource oriented. The two algorithms: EWMA and Leaky Bucket according to which provided use cases and test cases according to IoT devices. A verifier called Prover if was also mentioned which made the verification of models through online platforms easier. The paper provides a unique idea regarding battery exhaustion attack and provides measures against its prevention to an extent and claim its feasibility very well. However, the paper considers the battery as resource oriented which cannot be true always.

In a study published by Shakhov, et al. [23] in 2018**,** This paper presented a new type of battery attack like the Denial of service attack called Denial of Battery attack. The paper demonstrated algorithms and mathematical models accordingly and gave a brief similarity and differences between DoS and DoB. The paper initiated in finding a new type of attack related to sensors of a device battery. The paper focused more on the mathematical model rather than providing more information on DoB attacks.

In a study published by Lee, et al. [24] in 2020**,** This paper presented battery draining attack related protocols in which various aspects were showcased which included identifying the frames during receiving packets. The shared key must be protected in order to avoid such attacks. The theoretical experiments according to the above stated was also put forwarded.

In a study published by Li, W., Rentemeister, et al. [25] in 2020**,** The paper mentioned a new idea about introducing a battery twin using cloud for an efficient and robust BMS (Battery Management System). The paper dealt with various algorithms for SOC and SOH states of battery with proper experimentation. Providing a twin for the battery will result in reducing battery stress, reduced capacities and other problems related to battery. Hence a twin using cloud is indeed going to resolve the problem of traditional BMS.

In a study published by Woo, et al. [26] in 2013**,** The paper brought in a new idea about knowing about battery related information and storing it to an extent through a "Virtual Battery". The virtual battery contains all the information required to know in case the battery is going to fail in some case to have a backup action through the virtual machine by using its PID. The components involved are mainly discharger and virtual battery manager. The discharger contains a discharge thread through which the virtual battery mimics the battery. A process of virtualization takes place throughout the mechanism of applying the virtual battery in a particular virtual machine.

VI. METHODOLOGY

A. Participants

A study was conducted to know people's interest and experience with cloud as source of battery storage and also the population facing attacks needed to be analyzed. This study was conducted through Google forms which was circulated randomly since the study planned according to the availability need not require specific population but a population which uses mobile devices on daily basis. A total of 63 participants were involved in this survey (38 females and 25 males). The survey was conducted within the city limits of Mumbai and it involved no biased condition since adapting the technique of random sampling.

B. Materials

Google Forms were the source of the conducted survey. The population of the conducted survey was done out of convenience and availability therefore in the population maximum were students. The only criteria which was to be accomplished was to find out the population which had an average use of mobile device up to 4 hours on a daily basis.

C. Procedure

A google form which was chosen as a medium to conduct the survey was circulated by using the sampling technique of simple random sampling which involves an equal chance of in a population of inclusion which will help in having a fair opportunity to test the hypothesis. The Google Form was circulated for almost a week which resulted with a set of 63 responses.

VII. EXPERIMENT

The test scores of the hypothesis-oriented parameters were taken into consideration by performing Chi-Square test with a confidence level of 95 percent. The questions that was appropriate for our study was sorted out the survey results which may result in the impact of our hypothesis. The participant in the survey must go through the details of the device's battery and came across various question which provided an opinion towards their need for improvement in BMS in their respective devices. A distinguishing factor which was to be considered in the survey was to be chosen which was gender parameter to notice the difference in response values while performing the tests. A calculated value for the analysed values in accordance to the parameter oriented questions was further compared to a tabulated value by considering the degree of freedom as 5% according to which the rejection of null hypothesis could be impacted which is inversely proportional to alternate hypothesis.

One of the survey questions: Do you think cloud is a safe way of battery storage? Provided a calculated value of 0.6614 and other one: Have you faced any battery related attack using your device which lead to major damage on your devices? Provided a calculated value of 0.9448. These values were calculated by applying formulas which moved in accordance with the observed as well as expected values out of which a further calculation is required for expected values. These values were checked with a tabulated value of 3.84(having a confidence level of 95 percent).

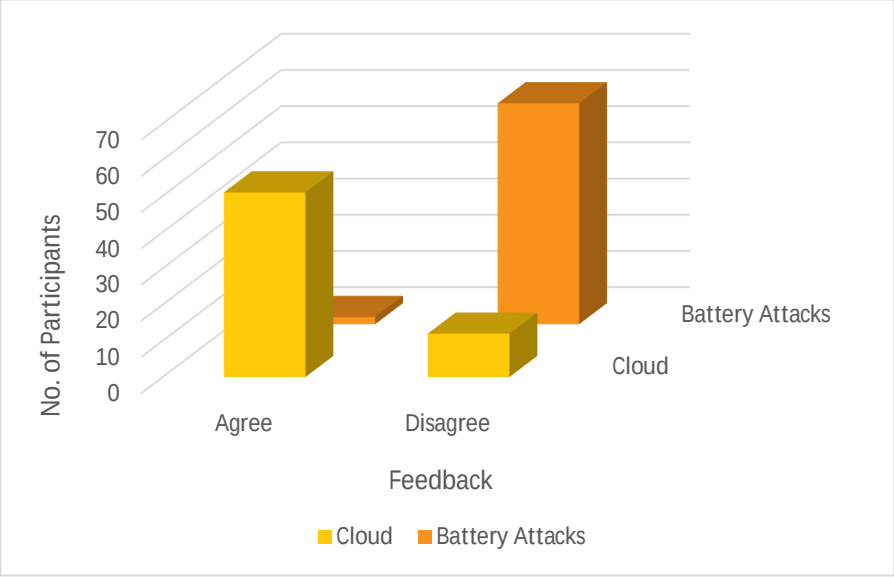


Fig. 1 The comparison of test values obtained through survey regarding i] Cloud ii] Battery Attacks

VIII. RESULTS

The test scores of the survey which was analysed and experimented on a random population on the basis of the specific parameters resulted that the population is likely to trust the cloud for battery storage since major population had been using it for critical storage purposes therefore if such a mechanism was implemented on fully furnished scale, the acceptance for such a technology would be majorly supported which is a big step towards proving H1.

The test scores in accordance with H2 could just provide some outcomes which supports the hypothesis. Since the participant's experiences in the arena of attacks was not specific a partial proof of the H2 is resulted. For the complete proof, the population must be specific, which provides a proper description of attacks out of which categorizing of attacks based on exfiltration could be done. The proper explanation of how the attack scenarios are present is provided in the section IV. Out of which readers may understand about the attack and then consider it for a survey which can be attributed to future work.

IX. LIMITATIONS AND FUTURE SCOPE

The survey conducted had a few noticeable limitations one of them being selection of population. The population if had been more specific then could have resulted in proper proof of whether the battery exfiltration is one of the most ignored and filthy attacks. The partial proof of the same could have been avoided in such a case. Although random distribution had given an equal opportunity to every sort of value, but the specificity is also one of the required factor. Due to limitation of time and access to the specific population this drawback was not excluded.

The idea about the mechanism of how cloud could work as a battery storage was stated but its mechanism still needs to be implemented. The proper implementation will only lead to better understanding the flaws and gains of the idea which was brought in. The acceptance of the stated idea is proved by the survey conducted. An experienced use will appropriately contribute to display the percentage of efficiency brought to the BMS by embedding a cloud system. Hence in future, an implementation of the same is expected along, which feasible enough for every mobile device by considering every factor that bring a major change in the device.

X. CONCLUSION

Battery is one of the critical components of a mobile device. Its efficiency is not only dependent on the health of device but also contributes to the energy level used which can contribute to knowledge about the resources used on proper basis. Excessive utilization of energy resources must not lead to their exhaustion hence an optimum and safe way must be adopted. Therefore, having an efficient BMS is of utmost importance.

Providing an alternative for battery is almost yet to be known but the approach to make a twin for it is possible through cloud computing since it's a strong source for storage and is proving its efficiency widespread in the recent years. Dependence of power for an over utilised component on an average basis is quite risky and hence a support system is crucial. In a long run one must also consider the device compatibility and evolve features according to user convenience and device capability to accomplish the features developed for ease of use and for resource friendliness. Not only by proving a support its damage is also a critical concern starting from where it is made. This scenario was highlighted in the performed study and hope these scenarios are well considered in future to accomplish a mission to provide an efficient battery management system.

XI. ACKNOWLEDGMENT

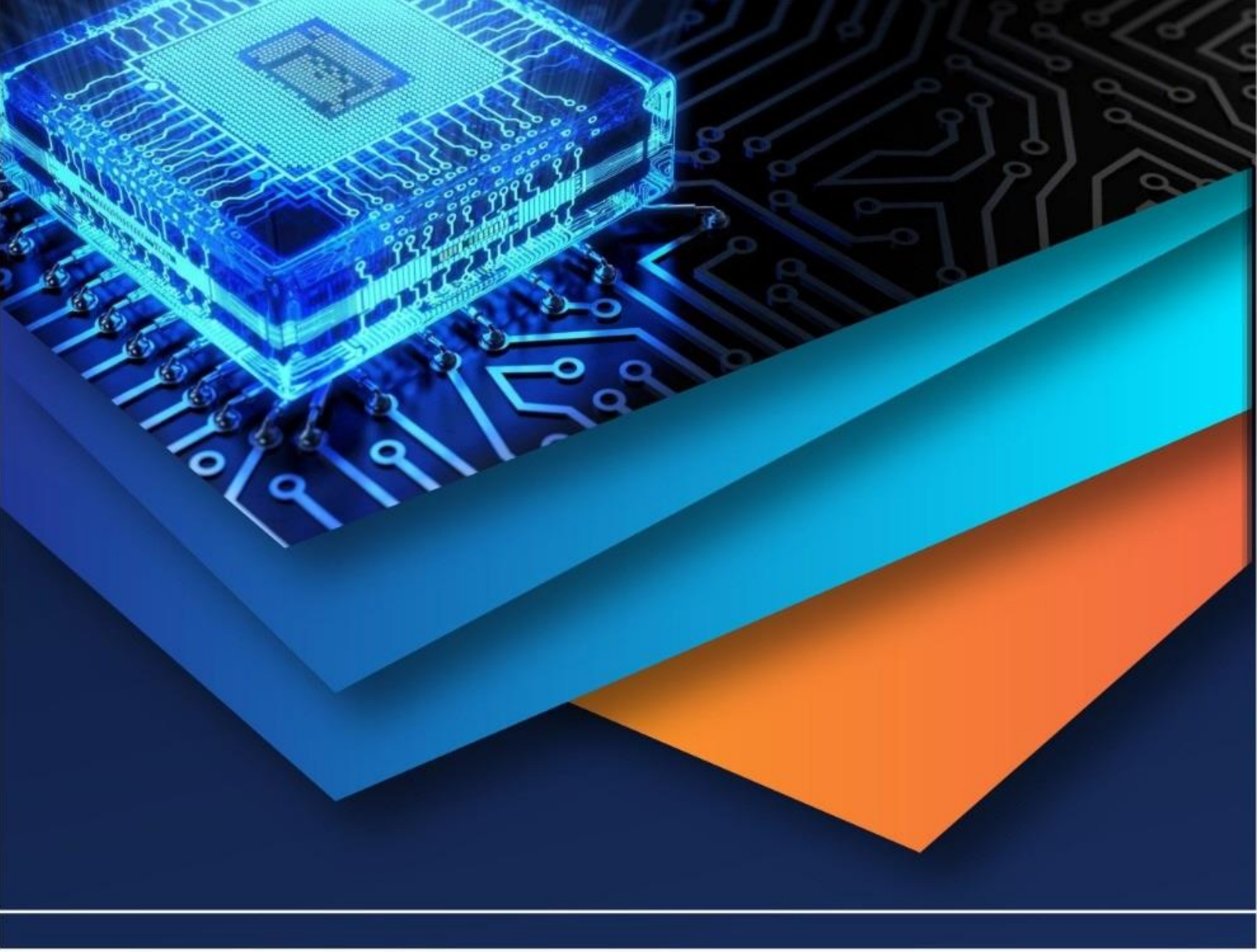
Sincere thanks and gratitude to Prof. Swapna Augustine Nikale, Department of Information Technology, B.K. Birla College of Arts, Science and Commerce, Kalyan for providing needful guidance in the work of this paper.

XII. GLOSSARY

1) *IoT:* Internet of things
2) *Wi-Fi:* Wireless Fidelity
3) *BMS:* Battery Management System
4) *DoS:* Denial of Service
5) *DoB:* Denial of Battery
6) *Chi-Square Test:* Non parametric test of independence used for comparison with categorical and associated variables
7) *API:* Application Programming Interface

REFERENCES

[1] Ferreira, D., Dey, A. K., & Kostakos, V. (2011). Understanding Human-Smartphone Concerns: A Study of Battery Life. Lecture Notes in Computer Science, 19–33. https://doi.org/10.1007/978-3-642-21726-5_2
[2] (US), D. J. J. M. T. N. (2017). SMARTPHONE CHARGING ALARM FEEDBACK DEVICE (US 9,569,949 B1). United States Patent.
[3] Ouyang, D., Liu, J., Chen, M., & Wang, J. (2017c). Investigation into the Fire Hazards of Lithium-Ion Batteries under Overcharging. Applied Sciences, 7(12), 1314. https://doi.org/10.3390/app7121314
[4] K. Lai, F. Cheng, S. T. Chou, Y. Chang, G. Wu and J. Tsai, "Any Charge: An IoT-Based Wireless Charging Service for the Public," in IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10888-10901, Dec. 2019, doi: 10.1109/JIOT.2019.2943030.
[5] Javed, A., Alyas Shahid, M., Sharif, M., & Yasmin, M. (2017). Energy Consumption in Mobile Phones. International Journal of Computer Network and Information Security, 9(12), 18–28. https://doi.org/10.5815/ijcnis.2017.12.03
[6] Ahmad, R. W., Bashir, R. S., Saeed, S., Lee, Y., Ko, K., & Son, Y. (2017). Online Cloud-Based Battery Lifetime Estimation Framework for Smartphone Devices. Procedia Computer Science, 110, 70–77. https://doi.org/10.1016/j.procs.2017.06.118
[7] Harish N1, Prashal V2 and Dr. D. Sivakumar 3, (2018). IOT Based Battery Management System, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 8 (2018) pp.
[8] Ravi, N., Scott, J., Han, L., & Iftode, L. (2008). Context-aware Battery Management for Mobile Phones. 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom), 17–21. https://doi.org/10.1109/percom.2008.108
[9] Lopez, A.B., Vatanparvar, K., Deb Nath, A.P. et al. A Security Perspective on Battery Systems of the Internet of Things. J Hardw Syst Secur 1, 188–199 (2017). https://doi.org/10.1007/s41635-017-0007-0
[10] Sajedifar, J., Nassiri, P., Monazzam, M. R., Shamsipour, M., & Ramezani, R. (2019). The effect of battery charge levels of Mobile phone on the amount of Electromagnetic waves emission. Journal of Environmental Health Science and Engineering, 17(1), 151–159. https://doi.org/10.1007/s40201-019-00336-3
[11] Kim, T., Makwana, D., Adhikaree, A., Vagdoda, J., & Lee, Y. (2018). Cloud-Based Battery Condition Monitoring and Fault Diagnosis Platform for Large-Scale Lithium-Ion Battery Energy Storage Systems. Energies, 11(1), 125. https://doi.org/10.3390/en11010125
[12] Lifshits, P., Forte, R., Hoshen, Y., Halpern, M., Philipose, M., Tiwari, M., & Silberstein, M. (2018). Power to peep-all: Inference Attacks by Malicious Batteries on Mobile Devices. Proceedings on Privacy Enhancing Technologies, 2018(4), 141–158. https://doi.org/10.1515/popets-2018-0036
[13] Li, S., Li, J., He, H., & Wang, H. (2019). Lithium-ion battery modelling based on Big Data. Energy Procedia, 159, 168–173. https://doi.org/10.1016/j.egypro.2018.12.046
[14] B. G. Schlicher, L. P. MacIntyre and R. K. Abercrombie, "Towards Reducing the Data Exfiltration Surface for the Insider Threat," 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, 2016, pp. 2749-2758, doi: 10.1109/HICSS.2016.345.
[15] Albugmi, Ahmed & Alassafi, Madini & Walters, Robert & Wills, Gary. (2016). Data Security in Cloud Computing. 10.1109/FGCT.2016.7605062.
[16] Fiore, U., Castiglione, A., De Santis, A., & Palmieri, F. (2017). Exploiting Battery-Drain Vulnerabilities in Mobile Smart Devices. IEEE Transactions on Sustainable Computing, 2(2), 90–99. https://doi.org/10.1109/tsusc.2017.2690148
[17] Ullah, F., Edwards, M., Ramdhany, R., Chitchyan, R., Babar, M. A., & Rashid, A. (2018). Data exfiltration: A review of external attack vectors and countermeasures. Journal of Network and Computer Applications, 101, 18–54. https://doi.org/10.1016/j.jnca.2017.10.016
[18] Wagh, K. S. (2018). A Survey: Data Leakage Detection Techniques. International Journal of Electrical and Computer Engineering (IJECE), 8(4), 2247. https://doi.org/10.11591/ijece.v8i4.pp2247-2253
[19] Ioulianou, P. P., Vassilakis, V. G., & Logothetis, M. D. (2019). Battery Drain Denial-of-Service Attacks and Defenses in the Internet of Things. Journal of Telecommunications and Information Technology, 2, 37–45. https://doi.org/10.26636/jtit.2019.131919
[20] Duh, Y.-S., Lin, K. H., & Kao, C.-S. (2018). Experimental investigation and visualization on thermal runaway of hard prismatic lithium-ion batteries used in smart phones. Journal of Thermal Analysis and Calorimetry, 132(3), 1677–1692. https://doi.org/10.1007/s10973-018-7077-2
[21] Jogendra Singh, Tanushri Mukherjee(2015). A Review Paper on Mobile Charging Using Microwaves International Journal of Scientific & Engineering Research, Volume 6, Issue 2
[22] Hristozov, Stefan & Huber, Manuel & Sigl, Georg. (2019). Protecting RESTful IoT Devices from Battery Exhaustion DoS Attacks.
[23] Shakhov, V., & Koo, I. (2018). Depletion-of-Battery Attack: Specificity, Modelling and Analysis. Sensors, 18(6), 1849. https://doi.org/10.3390/s18061849
[24] Lee, I.-G., Go, K., & Lee, J. H. (2020). Battery Draining Attack and Defense against Power Saving Wireless LAN Devices. Sensors, 20(7), 2043. https://doi.org/10.3390/s20072043
[25] Li, W., Rentemeister, M., Badeda, J., Jöst, D., Schulte, D., & Sauer, D. U. (2020). Digital twin for battery systems: Cloud battery management system with online state-of-charge and state-of-health estimation. Journal of Energy Storage, 30, 101557. https://doi.org/10.1016/j.est.2020.101557
[26] Woo, Y., Park, S. Y., & Seo, E. (2013). Virtual Battery: A testing tool for power-aware software. Journal of Systems Architecture, 59(9), 794–800. https://doi.org/10.1016/j.sysarc.2013.06.006
[27] https://blog.lukaszolejnik.com/exfiltrating-data-using-browser-battery-discharge-information/
[28] https://data-flair.training/blogs/software-virtualization/
[29] https://blog.lukaszolejnik.com/exfiltrating-data-using-browser-battery-discharge-information/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY