IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 10, Issue 1, January 2020, ||Series -VI|| PP 41-45

Smart Card Application Study for Future Internet of Things Development

Dr.Yogesh Kumar Sharma[1], Shamita Shivashankar Hiremath[2]
[1]*Research Guide, Associate Professor, Shri JJT University, Jhunjhunu, India*
[2]*Research Scholar, Shri JJT University, Jhunjhunu, India*
Received 14 January 2020; Accepted 30 January 2020

Abstract: Currently, the Internet of Things isn't the second Internet rather it's the network of devices that tend to be linked to the Internet that can be used each and every day to search Google, add images as well as link with friends. it's the network of Products that tend to be linked to the Internet, therefore they have their personal IP address and may link to every other to automate easy tasks. With regard to the Io T to be completely recognized just about all devices require being capable to link to every other, irrespective of exactly what company manufactured the Product or even that businesses have business relationships with every other. Within case of smart greeting card, there tend to be security factors that tend to be particular to smart credit cards as well as that require to be used into accounts when developing the safe smart card-based application.
Keywords*:* IOT, Smart Cards, Security Threat, Cryptographic Chip Architecture.

I. INTRODUCTION

The Internet of Things (IoT) is within its childhood. it has not really been completely developed and it is fragmented. Internet of Things Range, the group devoted to getting businesses together to accelerate the development of the IoT [1, 2], even comes close the current state of the IoT to the delivery of the computer, observing businesses as well as consumers are simply learning that Products may link to the Internet and today it's time to Figure away exactly what to perform with the Technology. "The current state of the Internet of Things is extremely fragmented, " Galvez described [3]. There will vary businesses as well as businesses that tend to be creating away their personal platforms with regard to either their customers or even their person requirements [4]. The true value of the Internet of Things doesn't place within the lights switching upon when the vehicle reaches the front yard, however rather the data that the linked devices gather regarding its customers. Picture the hospital with linked devices [5]. The data gathered through individuals devices results Information upon the standing of sufferers as well as operates analytics upon the numerous monitoring device, helping the hospital to operate as optimally as feasible [5, 6].

The selection of data through devices enables consumers, businesses as well as whole linked cities to operate more proficiently. Nevertheless, accumulating considerable amounts of data provides problems [7]. A few of the problems that nevertheless require to be Figured away tend to be partly around the algorithms that may process the data and provide a person something useful away of it, What exactly are a person actually getting of just about all this data you're accumulating? [8]

with the selection of data arrive major privateness as well as security issues with regard to consumers. Each Galvez as well as Jones agree that it's upward to the manufacturers of the Products to make sure they tend to be protecting person data [9]. Within General, the IoT encourages the heightened level of aWareness regarding the World, along with a platform that to monitor the reactions to the altering conditions that stated aWareness reveals all of us to. As well as, like the introduction of the Internet itSelf, the IoT allows variety applications which range from the micro to the macro, as well as through the insignificant to the Critical. Because we're concentrating here upon the reason why the IoT is essential [10], let's change the interest to the "macro" as well as the "Critical" first, and appear from a few attention grabbing ideas that tend to be already within development across the globe.

Through 2025, the IoT's financial impact might achieve US$11 trillion, or even 11% of global financial value, as well as through 2030 the IoT might impact almost the whole economic climate. From the Core of the IoT tend to be smart devices. They will be each and every form as well as size, through nanochips as well as smart dirt to huge devices. The number of linked points may grow exponentially through 15 billion within 2015 to two hundred billion within 2020 [11]. Nevertheless, whilst the IoT appears to be simply one Technology, it actually incorporates other major systems, this kind of as Cloud Computing, data analytics, mobile, devices, as well as machine-to-machine communications. The actual value of the IoT doesn't originate from just about all the connections it produces however through the data it generates. with real-time data analytics, the IoT becomes the live communications network with regard to promoting experience as well as

enhancements. it will even become the foundation of live business, by which businesses may be capable to sense as well as react to customers within the moment.

II. LITERATURE REVIEW

The Internet of Things pertains to the interrelated devices that can to transfer data on the network without needing computer as well as Human interaction devices. Internet of Things is actually directly as well as indirectly associated with everyday Lifestyle Products across the globe. Internet connectivity is actually one of the major needs of various application as it is actually anticipated to grow from high rate within following forecast time period [12].

Furthermore, internet connectivity demands much more monitoring via applications as well as Human interactions. Furthermore, Internet of Things offers a good easier as well as comfy Controlling of various electronic devices through one location. Internet of Things is actually definite as a hidden as well as smart network of points that match directly or even indirectly with every other that is fueling the enhancement throughout the forecast time period [13].

The ability to forecast, with fine-grained precision, the onset of conditions that market forest that will fire before they escape of Control as well as begin, permit containment teams to react faster as well as very first responders to quickly manage targeted evacuations. This exact same Concept is applicable similarly to the smarter recognition of as well as reaction to mudslides, avalanches, earthquakes as well as other organic disasters [14].

Cities as well as areas automating visitors management that successfully notices as well as governs the flow of visitors based upon ever-changing conditions; car parking applications that smartly guide vehicles to open up places, getting rid of wasted time as well as energy as well as dramatically reducing upon emissions; automating utility consumption, generation as well as distribution on the great scale, just about all with a watch to the mitigation of waste that much surpasses the capabilities of existing systems [15].

The IoT is actually allowing businesses to deliver much more proactive as well as interactive Products as well as services that enhance the brand encounter as well as customer devotion. Furthermore, businesses may use the IoT to enhance their Products as well as services as well as co-innovate with customers, whilst leftover continuously within touch with them to realize their altering requirements as well as desires [16]. The proceed through Products to services has been below method for a few time, however digitization may accelerate the transition, as the IoT enables businesses to much more directly function their customers. The IoT will even help businesses fulfill increasing customer demand with regard to live service. Businesses ought to make use of the possible offered through the IoT to create new services together the Product lifecycle to check out methods to produce services utilizing existing capabilities within the business.

III. IoT SECURITY ARCHITECTURE

The Internet of Things pertains to the interrelated devices that can to transfer data on the network without needing computer as well as Human interaction devices. Internet of Things is actually directly as well as indirectly associated with everyday Lifestyle Products across the globe. Internet connectivity is actually one of the major needs of various application as it is actually anticipated to grow from high rate within following forecast time period.

Furthermore, internet connectivity demands much more monitoring via applications as well as Human interactions. Furthermore, Internet of Things offers a good easier as well as comfortable Controlling of various electronic devices through one location. Internet of Things is actually definite as a hidden as well as smart network of points that match directly or even indirectly with every other that is fueling the enhancement throughout the forecast time period algorithms that Control devices tend to be becoming increasingly sophisticated. All of us already have Self-driving vehicles as well as Self-learning bots.

Through setting upward machine-to-machine communications as well as making algorithms that allow things as well as devices to Control every other, all of us may produce a new level of automation that may dramatically change the way you interact, work, as well as collaborate.

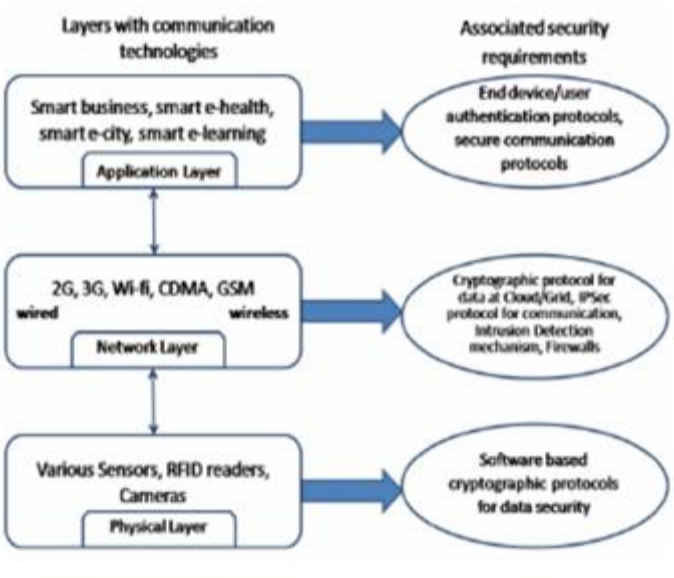

Fig. 1 IoT Security Architecture [12]

We will have many new interactions between individuals, points, as well as devices that today appear like Science fictional. Many of the points within our everyday lives in your own home as well as work may interact with every other, allowing all of us to make use of them within new methods. Within this linked World, getting entry to points like vehicles may become much more essential compared to having them.

From the Human-to-machine level, all of us may be capable to evaluate the standing of devices, obtain Warnings when they require upkeep, as well as Control their roles within Production from any kind of provided moment. The IoT will even allow all of us to Control robot plug-ins of the bodies, this kind of as substitutes with regard to dropped or even handicapped braches or even suits to enhance the power as well as other capabilities. As well as Humans as well as devices may work together as teams, interacting via the IoT. Utilizing the IoT, devices may organize as well as connect with other devices to produce big armies of automated robots able of acting together within swarms, as ants perform within nature. Devices will even be capable to monitor one another with regard to possible difficulties as well as perform maintenance without Human intervention.

IV. SMART CARD SECURITY THREATS

Invasive [4] attacks tend to be attacks that need the microprocessor inside a smart card to be eliminated as well as directly attacked via a physical means. This class of attacks may, from least within theory, give up the security of any kind of safe microprocessor. Nevertheless, these attacks typically need very costly gear along with a big investment within time to create results. Invasive attacks tend to be therefore regarded as to be mainly within the world of semiconductor manufacturers. Semi-invasive [6] attacks need the area of the notch to be subjected. An attacker then looks for to give up the security of the safe microprocessor without directly changing the nick. A few examples of this type of attack consist of watching the electromagnetic emanations utilizing a suitable probe as well as injecting problems utilizing laser light or even white light.

Non-Invasive [11] attacks look for to obtain Information without changing the smart greeting card, i.e. each the safe microprocessor as well as the plastic greeting card stay untouched. An attacker may try to obtain Information through watching Information that leakages throughout the calculation of confirmed command, or even try to provide problems utilizing systems other compared to light.

4.1 Chip Architecture

The surface of the chip utilized inside a smart card can be discovered by eliminating the plastic body of the card and make use of fuming nitric acid to take away the resin used to guard the microprocessor. When the chip has been open the easiest mode of analysis is to simply look at it under a microscope.

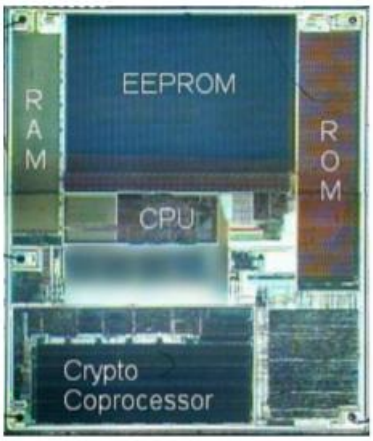

Fig.2 Chip Surface Architecture [15]

The dilemma of faults taking place in microprocessors has existed for a comparatively long time. One of the primary explanations of faults being incited in microprocessors was accidental. It was experiential that radioactive particles formed by elements naturally there in packaging material trigger faults in chips. For card/ chip testing we need to think about elements like- Supply Voltage, External Clock, Temperature, Electromagnetic flux, Cryptographic Algorithms. Additional to deal with attacks we require the countermeasures that can be utilize to guard microprocessors from fault attacks are based on technique earlier in use for integrity purposes. However, countermeasures only require to be applied in processes wherever an attacker could advantage from injecting a fault, even though a thorough study of a given application is necessitate to decide where countermeasures are requisite.

V. CONCLUSION

The IoT is inflowing a second wave that offer corporations the occasion to develop into live, digital businesses. Looking at methods that the IoT is being utilized nowadays, we can foresee a future where technology will be a part of nearly everything we do in business and private life. Suitable standardization on interoperability and security of smart cards has a significant influence in this development. There are also many options for placing M/Chip Advance based debit cards. Users can put their smart cards by cash or with their other payment cards by way of proprietary software POS machines which are to be found in some places.

REFERENCES

[1]. Ghosh, Shirsha, et al. "Swing-Pay: One Card Meets All User Payment and Identity Needs: A Digital Card Module using NFC and Biometric Authentication for Peer-to-Peer Payment." IEEE Consumer Electronics Magazine 6.1 (2017): 82-93.
[2]. Bakshi, Sana Zeba, et al. "Wireless E-Passport Using Smart Card Technology." (2017).
[3]. Hussain, S. Mahaboob, Prathyusha Kanakam, and A. S. N. Chakravarthy. "Inhibiting Cognitive Bias in Forensic Investigation Using DNA Smart Card with IOT." International Journal of Control Theory and Applications 10.14 (2017): 251-255.
[4].]Xiao, Juan, Juan Wub, and Donglai Xua. "Implementation of a secure USIM COS architecture for mobile payment applications." Proc. of SPIE Vol. Vol. 10322. 2017.
[5]. Felser, M. "Profinet Communication Card For The Cern Cryogenics Crate Electronics Instrumentation." (2017).
[6]. Grout, Ian, and Alexandre César Rodrigues da Silva. "RFID enabled sensor system design." Electrical Engineering Congress (iEECON), 2017 International. IEEE, 2017.
[7]. Jia, L. I. U., et al. "Implementation of IC Card Authentication Method Based on Self-defined Algorithm." DEStech Transactions on Engineering and Technology Research eeta (2017).
[8]. Karpinskyy, Bohdan, et al. "8.7 Physically unclonable function for secure key generation with a key error rate of 2E-38 in 45nm smart-card chips." Solid-State Circuits Conference (ISSCC), 2016 IEEE International. IEEE, 2016.
[9]. Ghosh, Shirsha, et al. "Swing-Pay: One Card Meets All User Payment and Identity Needs: A Digital Card Module using NFC and Biometric Authentication for Peer-to-Peer Payment." IEEE Consumer Electronics Magazine 6.1 (2017): 82-93.
[10]. Viji, C., et al. "Smart Vehicle Authentication and Due Date Monitoring System using IoT." Asian Journal of Applied Science and Technology (AJAST) 1.2 (2017): 265-267.

[11]. Courbon, Franck, Sergei Skorobogatov, and Christopher Woods. "Direct charge measurement in Floating Gate transistors of Flash EEPROM using Scanning Electron Microscopy." (2016).
[12]. Singhai, Anand, Rashmi A. Jain, and Siddharth Jain. "Wireless Emergency Response System for Town Planning and Public Sector using Smart Card/UID Card." IJETT 1.3 (2016).
[13]. Klengel, Sandy, et al. "Novel failure diagnostic methods for smart card systems." Electronics System-Integration Technology Conference (ESTC), 2014. IEEE, 2014.
[14]. Hussain, S. Mahaboob, Prathyusha Kanakam, and A. S. N. Chakravarthy. "Inhibiting Cognitive Bias in Forensic Investigation Using DNA Smart Card with IOT." International Journal of Control Theory and Applications 10.14 (2017): 251-255.
[15]. Bae, Won-il, and Jin Kwak. "Smart Card-Based Secure Authentication Protocol in Multi-Server IoT Environment." (2017).
[16]. Audouin, Maxime, Mohamad Razaghi, and Matthias Finger. "Can North-made IOT solutions address the challenges of emerging cities in the South? The case of Korean born Smart transportation card implementation in Bogota." 2016 International Tech4Dev Conference. No. EPFL-CONF-221073. 2016.
[17]. Effectual Secured approach for Internet of Things with Fog Computing and Mobile Cloud Architecture Using IFogSim, P S, YK Sharma, WCE-2019 - London - U. K., 101-104
[18]. A Pragmatic Evaluation of Stress and Performance Testing Technologies for Web Based Applications, P sonkari, DYK Sharma, IEEE, Amity International Conference on Artificial Intelligence
[19]. Significance Study of User Web Access Records Mining For Business Intelligence, AD Vyas, DYK Sharma, Indian Journal of Applied Research (IJAR) 9 (7), 10-13
[20]. Designing Hybrid Data Mining Technique for Efficient industrial Engineering Domain , DYK Sharma, Kumari, Sunita, Journal of Computational Information Systems 15 (3), 128-136

Dr.Yogesh Kumar Sharma, etal. "Smart Card Application Study for Future Internet of Things Development". *IOSR Journal of Engineering (IOSRJEN)*, 10(1), 2020, pp. 41-45.