American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-6, Issue-9, pp-196-202
www.ajer.org
Research Paper Open Access

Smart Card: The Turning Point of Technology as a Solution to Africa Problems.

[1]Ebole Alpha, [2]Iluno Christiana and [3]Kuyoro S.O
[1]Computer Science Department, School of Technology, Lagos State Polytechnic, Lagos State, Nigeria.
[2] Department of Mathematics and Statistics, Lagos State Polytechnic, Lagos State Nigeria
,[3]Computer Science Departments, Babcock University, Ogun State, Nigeria.
*Corresponding Author: *Ebole Alpha F*

Abstract: *Integrated Circuit Cards have conventionally come to be known as "Smart cards". A smart card is a card that is embedded with either a microprocessor and a memory chip or only a memory chip with non-programmable logic. The microprocessor card can add, delete, and otherwise manipulate information on the card, while a memory-chip card can only undertake a pre-defined operation.*

The fabrication of the card involves manufacturing of substrate which contains the chip called a COB (Chip On Board) and consists of a glass epoxy connector board on which the chip is bonded to the connectors. A typical smartcard consists of an 8-bit microprocessor running at approximately 5 MHz with ROM, EEPROM and RAM, together with serial input and output, all in a single chip that is mounted on a plastic carrier. The operating system is typically stored in ROM, the CPU uses RAM as its working memory, and most of the data is stored in EEPROM. One of the most common smart card operating environments is Java. Java-enabled smart cards are called Java Cards13

The Java community has developed a wide and strong base security and safety issue, which can be leveraged when developing smart-card applications. Java Card platform provides a secure execution environment with a "firewall" between different applications in the same card. Encryption and decryption of data are performed on request by the card chipset itself. In this way, the user's private key is kept secure and cannot be eavesdropped. Thus, chip cards have been the main platform for holding a secure digital identity.

Keywords: *memory chip, microprocessor card, Encryption and decryption*

I. Introduction

The International Organization for Standardization (ISO) standard 7810 "Identification Cards – Physical Characteristics" defines physical properties such as flexibility, temperature resistance, and dimensions for three different card formats (ID-1, ID-2, and ID-3). There are different types of ID-1 format cards, each specified by a different substandard.

Integrated Circuit cards **(smart cards)** are the newest and belong to the ID-1 family, and these types of cards allow far greater orders of enormity in terms of data storage – cards with over 20 Kbytes of memory are currently available and the stored data can be protected against unauthorized access and tampering. Memory functions such as reading, writing, and erasing can be linked to specific conditions, controlled by both hardware and software. Smartcards are more reliable and have longer expected lifetimes over magnetic stripe cards. Integrated Circuit Cards have conventionally come to be known as "Smart cards". A smart card is a card that is embedded with either a microprocessor and a memory chip or only a memory chip with non-programmable logic. Memory Cards: though often also referred to as smartcards, memory cards are typically much less expensive and much less functional than microprocessor cards. They contain EEPROM and ROM memory, as well as some address and security logic. In the simplest designs, logic exists to prevent writing and erasing of the data. More complex designs allow for memory read access to be restricted. Since they cannot directly manipulate data they are dependent on the card reader (also known as the card-accepting device) for their processing and are suitable for uses where the card performs a fixed operation. Typical memory card applications are pre-paid telephone cards and health insurance cards.

Historical development

An important patent for smart cards with a microprocessor and memory as used today was filed by Jürgen Dethloff in 1976 and granted as USP 4105156 in 1978 In 1977, Michel Ugon from Honeywell Bull invented the first microprocessor smart card with two chips: one microprocessor and one memory, Three years later, Motorola used this patent in its "CP8". In 2001, Bull sold its CP8 division together with its patents to Schlumberger, who subsequently combined its own internal smart card department and CP8 to create Axalto. In 2006, Axalto and Gemplus, at the time the worlds top two smart card manufacturers, merged and became Gemalto. In 2008 Dexa Systems spun off from Schlumberger and acquired Enterprise Security Services business, which included the smart card solutions division responsible for deploying the first large scale public key infrastructure (PKI) based smart card management systems. The first mass use of the cards was as a telephone card for payment in French pay phones, starting in 1983

Europay MasterCard Visa (EMV)-compliant cards and equipment are widespread. The United States started using the EMV technology in 2014. Typically, a country's national payment association, in coordination with MasterCard International, Visa International, American Express and Japan Credit Bureau (JCB), jointly plan and implement EMV systems. Historically, in 1993 several international payment companies agreed to develop smart-card specifications for debit and credit cards. The original brands were MasterCard, Visa, and Europay. The first version of the EMV system was released in 1994. In 1998 the specifications became stable.

EMVCo maintains these specifications. EMVco's purpose is to assure the various financial institutions and retailers that the specifications retain backward compatibility with the 1998 version. EMVco upgraded the specifications in 2000 and 2004. EMV compliant cards were first accepted into Malaysia in 2005 and later into United States in 2014. MasterCard was the first company that has been allowed to use the technology in the United States. The United States has felt pushed to use the technology because of the increase in identity theft. The credit card information stolen from Target in late 2013 was one of the largest indicators that American credit card information is not safe. Target has made the decision on April 30, 2014 that they are going to try and implement the smart chip technology in order to protect themselves from future credit card identity theft. Before 2014, the consensus in America was that there was enough security measures to avoid credit card theft and that the smart chip was not necessary. The cost of the smart chip technology was significant, which was why most of the corporations did not want to pay for it in the United States. The debate came when online credit theft was insecure enough for the United States to invest in the technology. The adaptation of EMV's increased significantly in 2015 when the liability shifts occurred in October by the credit card companies.

Research methodology

The whole operation starts with the application requirements specification. From the requirements individual specifications can be prepared for the chip, card, mask ROM software and the application software. The ROM software is provided to the semiconductor supplier who manufactures the chips. The card fabricator embeds the chip in the plastic card. It is also quite normal for the fabricator to load the application software and personalization data. Security is a fundamental aspect in the manufacture of a smart card and is intrinsic to the total process.

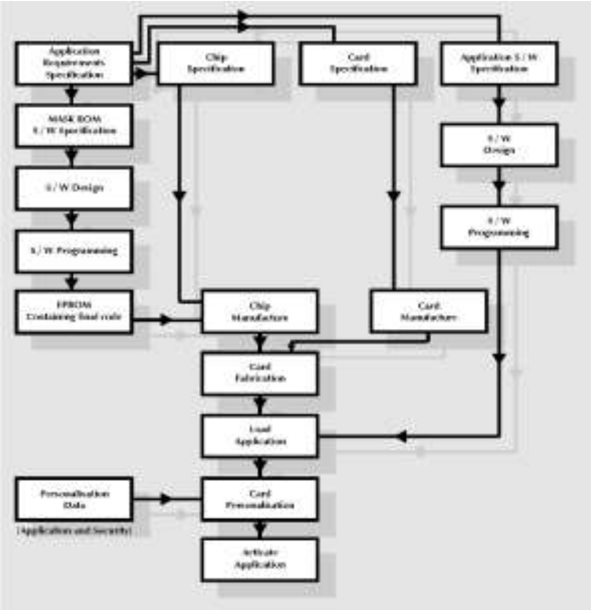


Figure 1: Stages in the manufacture of a Smart Card

Chip specification

The key parameters for the chip specification are Microcontroller type (e.g 6805, 8051), Mask ROM size, RAM size, Non volatile memory type (e.g EPROM, EEPROM), Non volatile memory size, Clock speed (external, and optionally internal), Electrical parameters (voltage and current) Communications parameters (asynchronous, synchronous, byte, block), Reset mechanism, Sleep mode (low current standby operation), Co-processor (e.g for public key cryptography)

Card specification

The specification of a card involves parameters that are common to many existing applications using the ISO ID-1 card. The following list defines the main parameters that should be defined, such as the Card dimensions, Chip location (contact card), Card material (e.g PVC, ABS), Printing requirements, Magnetic stripe (optional), Signature strip (optional), Hologram or photo (optional), Embossing (optional) and Environmental parameters. The choice of chip location has been a difficult subject due largely to the use of magnetic stripes. The early French cards put the IC module further off the longitudinal axis of the card than the standard eventually agreed by ISO. This was preferable because of the residual risk of chip damage due to bending. PVC was traditionally used in the manufacture of cards and enabled a higher printing resolution. Such cards are laminated as three layers with transparent overlays on the front and back. More recently ABS has been used which allows the card to be produced by an injection moulding process.

Mask ROM Specification

The mask ROM contains the operating system of the smart card. It is largely concerned with the management of data files but it may optionally involve additional features such as cryptographic algorithms (e.g DES). This part of the card development process is clearly specific to the particular application. The application code could be designed as part of the mask ROM code but the more modern approach is to design the application software to operate from the PROM non volatile memory. This allows a far more flexible approach since the application can be loaded into the chip after manufacture. More over by the use of EEPROM it is possible to change this code in a development environment. The manufacturer of a chip with the user's ROM code takes on average three months. Application code can be loaded into the PROM memory in minutes with no further reference to the chip manufacturer.

Chip Fabrication

The fabrication of the card involves a number of processes as shown in figure 2 below. The first part of the process is to manufacture a substrate which contains the chip. This is often called a COB (Chip On Board) and consists of a glass epoxy connector board on which the chip is bonded to the connectors. There are three technologies available for this process, wire bonding, flip chip processing and tape automated bonding (TAB). In each case the semiconductor wafer manufactured by the semiconductor supplier is diced into individual chips. This may be done by scribing with a diamond tipped point and then pressure rolling the wafers so that it fractures along the scribe lines. More commonly the die is separated from the wafer by the use of a diamond saw. A mylar sheet is stuck to the back of the wafer so that following separation the dice remain attached to the mylar film.

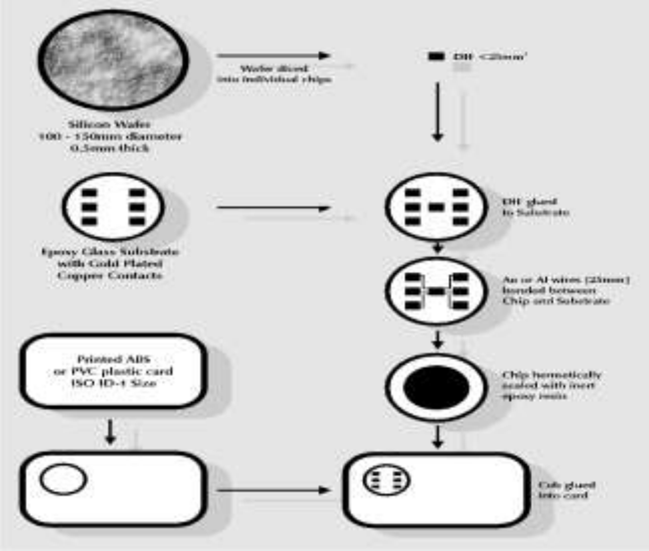
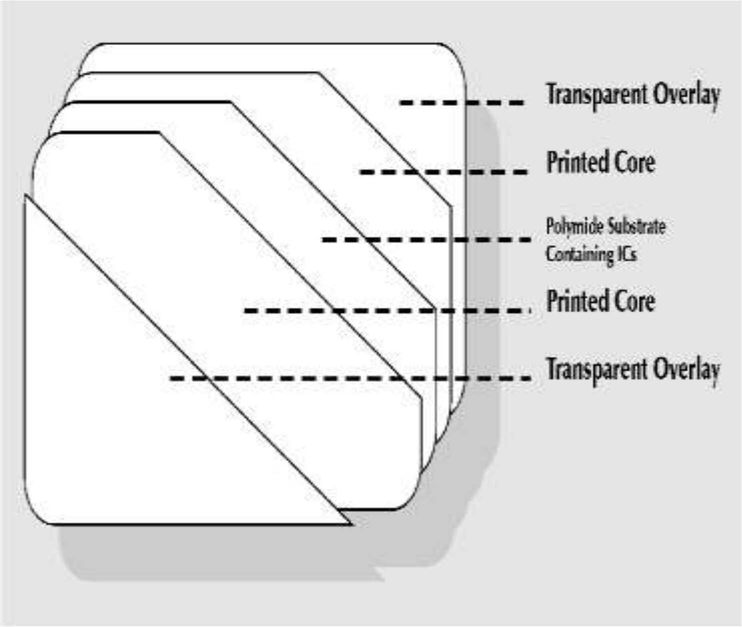


Figure 2: Chip Fabrication

Wire bonding is the most commonly used technique in the manufacture of smart cards. Here a 25uM gold or aluminium wire is bonded to the pads on the chip using ultrasonic or thermo compression bonding. Thermo compression bonding requires the substrate to be maintained at between 150C and 200C or maximum 350C and allow only 5 or 6 wires to be bonded for smart card applications. However in the semiconductor industry generally two other techniques are used, the flip chip process and tape automated bonding. In both cases gold bumps are formed on the die. In flip chip processing the dice are placed face down on the substrate and bonding is affected by solder reflow. With tape automated bonding the dice are attached by thermo-compression to copper leads supported on a flexible tape similar to a 35mm film. The finished substrate is hermetically sealed with an inert material such as epoxy resin. The complete micro-module is then glued into the card which contains the appropriately sized hole. The fabrication of a contactless card is somewhat different since it always involves a laminated card as shown in figure 3. The ICs and their interconnections as well as the aerial circuits are prepared on a flexible polyimide substrate.



Application load

Assuming the application is to be placed in the PROM memory of the IC then the next stage in the process is to load the code into the memory. This is accomplished by using the basic commands contained in the operating system in the mask ROM. These commands allow the reading and writing of the PROM memory.

Card Personalisation

The card is personalized to the particular user by loading data into files in the PROM memory in the same way that the application code is loaded into memory. At this stage the security keys will probably be loaded into the PROM memory and to enable the application for operation, it will involve the setting of flags in the PROM memory that will hold back any further changes to be made to the PROM memory except under direct control of the application. One of the most common smart card operating environments is Java. Just as in the Java operating environment for computer systems, the Java Card API enables a “Write Once, Run Anywhere” approach, by wrapping proprietary, vendor-dependant API and system calls into a common framework. Using OOP has obvious benefits for security, allowing the developer to encapsulate sensitive data and algorithms within objects. Java Card platform provides a secure execution environment with a “firewall between different applications in the same card. This allows different applications on the same card to function separately and independently from each other as if they were on separate cards.

II. RESULT

Cryptographic Capabilities, is the current state of the art smartcards have sufficient cryptographic capabilities to support popular security applications and protocols, because it provides elliptic curve algorithms which is a strong security without the need for large integer. RSA signatures and verifications are supported with a choice of 512, 768, or 1024 bit key-lengths. The algorithms typically use the Chinese Remainder Theorem (CRT) in order to speed up the processing. Even at the 1024 bit key-length, the time needed to perform a signature is typically under one second. Usually the EEPROM file that contains the private key is designed such that the sensitive key material never leaves the chip. Even the card holder can't access the key material in this case. The usage of the private key is protected by the user's PIN, so that possession of the card does not imply the ability to sign with the card.

Application examples

Web Browsers (SSL, TLS) Web browsers use technology such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide security while browsing the World Wide Web. These technologies can authenticate the client and/or server to each other and also provide an encrypted channel for any message traffic or file transfer. The authentication is enhanced because the private key is stored securely on the smartcard. The encrypted channel typically uses a symmetric cipher where the encryption is performed in the host computer because of the low data transfer speeds to and from the smartcard.

Secure Email (S/MIME, OpenPGP)

S/MIME and OpenPGP allow for email to be encrypted and/or digitally signed. As with SSL, smartcards enhance the security of these operations by protecting the secrecy of the private key and also unwrapping session keys within a security perimeter. Web based HTML forms can be digitally signed by your private key. This could prove to be a very important technology for internet based business because it allows for digital documents to be hosted by web servers and accessed by web browsers in a paperless fashion. Online expense reports, W-4 forms, purchase requests, and group insurance forms are some examples. For form signing, smartcards provide portability of the private key and certificate as well as hardware strength non repudiation.

Object Signing

If an organization writes code that can be downloaded over the web and then executed on client computers, it is best to sign that code so the clients can be sure it indeed came from a reputable source. Smartcards can be used by the signing organization so the private key can't be compromised by a rogue organization in order to impersonate the valid one.

Kiosk / Portable Preferences

Certain applications operate best in a "kiosk mode" where one computer is shared by a number of users but becomes configured to their preferences when they insert their smartcard. The station can then be used for secure email, web browsing, etc. and the private key would never leave the smartcard into the environment of the kiosk computer. The kiosk can even be configured to accept no mouse or keyboard input until an authorized user inserts the proper smartcard and supplies the proper PIN.

File Encryption

Even though the 9600 baud serial interface of the smartcard usually prevents it from being a convenient mechanism for bulk file encryption, it can enhance the security of this function. If a different, random session key is used for each file to be encrypted, the bulk encryption can be performed in the host computer system at fast speeds and the session key can then be wrapped by the smartcard. Then, the only way to easily decrypt the file is by possessing the proper smartcard and submitting the proper PIN so that the session key can be unwrapped.

Workstation Logon

Logon credentials can be securely stored on a smartcard. The normal login mechanism of the workstation, which usually prompts for a username and password, can be replaced with one that communicates to the smartcard.

Dialup Access (RAS, PPTP, RADIUS, TACACS)

Many of the common remote access dial-up protocols use passwords as their security mechanism. As previously discussed, smartcards enhance the security of passwords. Also, as many of these protocols evolve to support public key based systems, smartcards can be used to increase the security and portability of the private key and certificate.

Payment Protocols (SET)

The Secure Electronic Transactions (SET) protocol allows for credit card data to be transferred securely between customer, merchant, and issuer. Because SET relies on public key technology, smartcards are a good choice for storage of the certificate and private key.

Digital Cash

Smartcards can implement protocols whereby digital cash can be carried around on a smartcard. In these systems, the underlying keys that secure the architecture never leave the security perimeter of hardware devices. Mondex18, VisaCash19, EMV (Europay-Mastercard- Visa), and Proton20 are examples of digital cash protocols designed for use with smartcards.

Building Access

Even though the insertion, processing time, and removal of a standard smartcard could be a hassle when entering a building, magnetic stripe or proximity chip technology can be added to smartcards so that a single token provides computer security and physical access.

Law-strong digital signatures

New digital signature laws are being written by many states that make it the end user's responsibility to protect their private key. If the private key can never leave an automatically PIN disabling smartcard, then the end user can find it easier to meet these responsibilities. Certificate authorities can help in this area by supporting certificate extensions that specify the private key was generated in a secure environment and has never left the confines of a smartcard. With this mechanism, higher levels of non-repudiation can be achieved when verifying a smartcard based signature while using a certificate containing such an extension. In other words, a digital signature carries more weight if its associated certificate validates that the private key resides on a smartcard and can never be extracted.

Security Evaluation of Smart Cards

Security Design Standards

The ultimate goal of smart card security is proven robustness and correct functioning of every single card delivered to the card user. Chip security and card life cycle security are the key links in this chain. Chip and card life cycle security are non-competitive issues which means that these properties should not and cannot be separated in the design process. The market for smart cards is highly cost sensitive; differences of a few cents per card matter when millions of units are involved. This means that any defensive measures must meet very stringent cost effectiveness tests that are unusual with other IT products. Attacks that involve multiple parts of a security system are difficult to predict and model. If cipher designers, software developers, and hardware engineers do not understand or review each other's work, security assumptions made at each level of a system's design may be incomplete or unrealistic. As a result, security faults often involve unanticipated interactions between components designed by different people. For example, National Institute of Standard and Technology (NIST) emphasizes the importance of computer security awareness and of making information security a management priority that is communicated to all employees.

Smart Card Security Evaluation

Currently, Financial Payment Systems, i.e. credit card brands, individually do smart card evaluations – un-standardized, possibly conflicting. Vendor's products may be subject to conflicting requirements, repeated and expensive evaluations by different users. ISO 15408 – Common Criteria for Information Technology Security Evaluation, the "CC", represents the outcome of efforts to develop criteria for evaluation of IT security that are widely useful within the international community. It is an alignment and development of a number of source criteria: The existing European, US, and Canadian criteria (ITSEC, TCSEC and CTCPEC respectively). The Common Criteria resolves the conceptual and technical differences between the source criteria. It is a contribution to the development of an international standard, and opens the way to worldwide mutual recognition of evaluation results. If independent third party evaluation should become mandatory, it would require sharing test methods and information about vulnerabilities between private companies and independent institutions. A public acceptance of an evaluation scheme could even require an open discussion and disclosure of information about risks and vulnerabilities to the public. It is therefore unfortunate if smart card security really depends on confidentiality of CPU design and specifications.

Common Criteria established an handful of important concepts in security system evaluations:

There should be a common structure and language for expressing product or system IT security requirements. There should be "catalogs" of standardized IT security requirement components and packages. The CC presents requirements25 for the IT security of a product or system under the distinct categories of functional requirements and assurance requirements. The CC functional requirements define desired security behavior. Assurance requirements are the basis for gaining confidence that the claimed security measures are effective and implemented correctly.

The CC envisages the definition of Protection Profile (PP), standardized and well understood sets of implementation independent security requirements developed by a user group to specify their security functionality needs for a particular product. This allows a manufacturer or product developer to build a product according to the requirements of a PP. They can then have it evaluated and claim conformance to the PP. The product is still evaluated against a security target (ST) but the contents of the ST mirror the requirements laid down in the PP. A security target is created by the product vendor and is therefore implementation specific. The smart card protection profile presented in this study is a joint effort of the Smart Card Security User Group (SCSUG). SCSUG is a global financially oriented industry group formed specifically to represent the security needs of the user community. It comprises of American Express, Europay, JCB, MasterCard, Mondex, Visa, NIST and NSA. As most readers surely know, before Common Criteria development one of the most accepted security standards was ITSEC (which served as a basis for the CC themselves).

The advantage of the second important concept in CC is that the security functionality will be expressed in an explicit, unambiguous way. The wording is well understood and includes detailed guidance for interpretation and application. The first important concept in CC makes comparison of certifications by users and mutual recognition by certification bodies more practical. The detailed guidance in CC on calculating attack potential aims at removing some of the subjectivity from this difficult assessment task and it may offer more clarity than the ITSEC. The Smart Card Security User Group protection profile emphasizes that a vulnerability to certain types of threats can only be ascertained by examining the IC, operating system and applications as an integrated whole because effective security relies on a synergistic contribution of these three layers. It was further noted in the same study that all the examined ITSEC certifications claimed a high Strength of Mechanisms (SoM) but the scope of each evaluation was also limited in some way, either to particular phases of the card life cycle, by exclusion of the chip from the Target of Evaluation or by specifically excluding relevant threats. It can be questioned whether a high SoM would have been attained if all threats were considered in the context of the integrated product, as it is issued to the user in its actual mode of use.

III. CONCLUSION

Most of the card systems in employment these days serve one motive and are associated with just one procedure or is hardwired in only one function. A smart card may not justify its subsistence in this area. The approach of prospect smart card is therefore to designing multi-application smart cards with individual operating structure bottomed on the open principle that can do a variety of applications. It must be programmable and configurable and it should be able to acclimatize to new requirements and new situations especially in regions such as operating system, memory management, and security.

REFERENCES

[1]. "ISO/IEC 7816-2:1999/Amd 1:2004 - Assignment of contacts C4 and C8". www.iso.org. Retrieved 2015-08-20.

[2]. Multi-application Smart Cards. Cambridge University Press.http://sipwebsrch02.si.edu/search?site=americanhistory&client=americanhistory&proxystylesheet=americanhistory&output=xml_no_dtd&filter=0&q=roland+moreno&submit.x=13&submit.y=8&s=SS

[3]. "Monticello Memoirs Program". Computerworld honors. Retrieved 13 February 2012.

[4]. "history of smartcard invention". Retrieved 29 July 2016.

[5]. "Taalkeuze/Choix de langue fedict.belgium.be". Eid.belgium.be. Retrieved 2014-02-13.

[6]. "Emergency Response Official Credentials: An Approach to Attain Trust in Credentials across Multiple Jurisdictions for Disaster Response and Recovery". January 3, 2011.

[7]. "OMA Newsletter 2007 Volume 2". Retrieved March 20, 2012.

[8]. Martin, Christophe (30 June 2010). "Update from SIM alliance on SCWS". Retrieved March 20, 2012.

[9]. "OMA Smart Card Web Server (SCWS)". Retrieved March 20, 2012.

[10]. "Smartcare go". Retrieved 24 September 2012.

[11]. Bar-El, Hagai. "Known Attacks Against Smartcards" (PDF). Discretix Technologies Ltd. Retrieved February 20, 2013.

Ebole Alpha F. "Smart Card: The Turning Point of Technology as a Solution to Africa Problems." American Journal of Engineering Research (AJER), vol. 6, no. 9, 2017, pp. 196–202.