Security Aspects in Internet and Mobile Communication

Pratik P. Watwani
Computer Engineering Department
Vivekanand Education Society's Institute of Technology
Mumbai, India.

***Abstract*—Internet and Mobile are an essential part of our daily lives. However, with the growth it has become more difficult to manage our privacy and security online. As the technology advances the underlying infrastructure and technologies that make the internet work and secured become highly complex. This paper discusses some of the difficulties faced on the internet and mobile communication systems, the ambush of the online attacks, their statistical data aspects, as well as some measures of securing the internet and mobile networks.**

***Keywords*—internet, mobile, security,mobile devices,cryptography,encryption, security systems.**

I. INTRODUCTION

As the technology has advanced in the span of years, a number of new inventions have been developed in the field of Internet and Mobile communication systems. From Analog Cellular Networks (1G) to Native IP networks(4G) communication has gained speed, optimization and reliability. Underneath the development over these new technologies lie the design specifications and the physical and logical properties that define the capabilities and limitations of communication networks.

When optically canvassing traditional e-commerce, the lack of security and a high caliber of fraud is optically discerned as the major impediment to people embracing the possibilities and advantages e-commerce can offer.

Different services are employed with different security measures, like, Web browsers are enabled to use public-key infrastructures for cryptographic key distribution and to use cryptographic protocols. Infelicitously, communication security alone is not enough. The magnification of the cyber world gave elevate to many paramount accommodations accessible to anyone with a connection. One of these consequential accommodations is digital communication. While this accommodation sanctioned us to communicate with others through the cyber world, this additionally sanctioned the communication with malignant users. While malignant users often utilize the cyber world for personal gain, this may not be constrained to financial/material gain. This is especially a concern to parents and children, as children are often targets of these maleficent users. Prevalent threats to personal safety include:

This paper discusses the feasibility of implementing security in internet and mobile communication systems. To achieve these security solutions, it is important to recognize the particular aspects of internet and mobile networks and properties and the conditions in which they shall be used. While some aspects make the security design easier the other aspects make it difficult to be implemented.

II. SECURITY IN INTERNET AND MOBILE COMMUNICATION

The fundamental building blocks of security in communication is often described in terms of confidentiality, integrity, authentication and nonrepudiation of dispatched data. These security accommodations are in turn implemented by sundry mechanisms that are conventionally cryptographic in nature.

As the technology advances, the threat level increases. In the past few years' internet and mobile have become an essential and consequential need in a quotidian life and hence a good target for hackers. There is confidentiality of traffic, of location, and of the communicating parties address, all of which are consequential for privacy.

Just like computers, all smartphones and internet networks are preferred targets of attacks. These assailments exploit impuissance's that can emanate from the expedient of communication like Concise Message Accommodation (SMS), Multimedia Messaging Accommodation (MMS), Wi-Fi networks, Email, Software, Bluetooth, Pictures, Videos GSM, the de facto ecumenical standard for mobile communications etc.

The main components while engendering a secure network is flexibility, reliability and congruous functionality. What is always ignored is that there is a tradeoff between security and other factors.

Web Browser and The operating system are more vulnerably susceptible to attacks and cause rigorous damage to the security resulting in the intrusion of malware and Trojans in the physical and logical properties which rely on impuissant cognizance of average users.

III. SECURITY ATTACKS

A. The goal of online attacks

Smartphones, or mobile phones connected with web; with advanced capabilities like those of personal computers (PCs), are appearing in more people's pockets. Online communication popularity and relatively lax security have made them captivating targets for attackers.

In 2011 it was visually perceived that, smartphones outsold PCs for the first time, and assailers have been exploiting this expanding market by utilizing old techniques along with incipient ones [1]. One example is the Valentine's Day attack (in 2011), in which assailants distributed a mobile picture sharing application that furtively sent premium-rate instant messages from the client's cellular phone.

One study found that, from 2009 to 2010, the number of incipient susceptibilities in mobile operating systems jumped 42 percent. [2] The number and sophistication of attacks on mobile phones is incrementing and countermeasures are slow to catch up. Smartphones and personal digital assistants (PDAs) give users mobile access to email, the cyber world, GPS navigation, and many other.

Be that as it may, cell phone security has not kept pace with conventional PC security. Specialized efforts to establish safety, for example, firewalls, antivirus, and encryption, are capricious on cell telephones, and cellular telephone working frameworks are not upgraded as much of the time as those on PCs. [3]

Mobile social networking applications sometimes lack the detailed privacy controls of their PC counterparts. Haplessly, many smartphone users do not apperceive these security shortcomings. Numerous clients neglect to empower the security programming that accompanies their phones, and they trust that surfing the digital world on their phones is as sheltered as or more secure than surfing on their PCs. [4]

Then, cellular telephones are turning out to be increasingly profitable as focuses for assault. Individuals are using cell phones for an increasing number of exercises and frequently store touchy information, for example, email, schedules, contact data and passwords, on the gadgets.

The thought processes behind online attacks are changed. You had stuff to purloin, your invention/property could be accustomed to show publicity or telecast spam, or possibly you just neglected to overhaul the security measures and your absent mindedness could delight the exhausted wishes of an inquisitive script-kiddie — one of those reasons is the reason we are hacked.

Each gadget and a system can accommodate an imply: to hold delicate information, or at any rate, give utilizable assets to send spam or attack different targets.

Geoff Livingston, Author and President of Tenacity5 Media quoted "**CYBERWAR IS THE BATTLEFIELD NOW**".

B. How an attack over internet and mobile communication occur ?

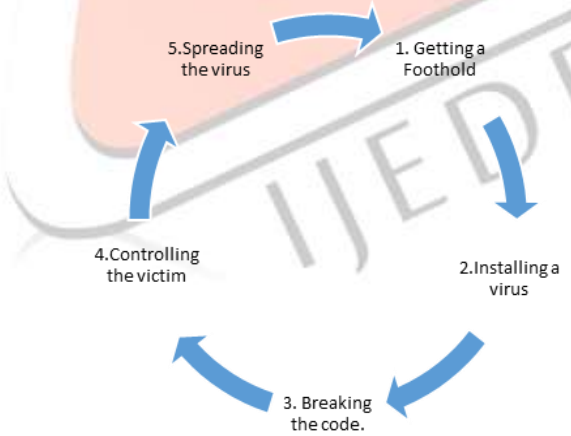

FIG 1. PROCESS FLOW OF ATTACK OVER WEB AND MOBILE NETWORKS.

The basic philosophy of an attack is broken into the 5 stages: [5]

1. Getting a Foothold: Wherein the hacker sends an infected email or a call or a sms. These are often spams like lottery's, free gifts, etc. this grabs the attention of the user and makes it vulnerable and the prey falls to it.
2. Installing a virus using emails, programs, mms websites etc. virus definitions are stored in these files using different mechanisms and are sent to the victim.
3. Breaking the code is the next step wherein the confidential data of victim is obtained using cracking software and thus accessing the entire data.
4. This step involves gaining the control of victim's behavior. Since the data is accessible to the hacker using the rootkit and other tools the hacker can control all the data and system.
5. As the hacker/attacker has received the control of the system, the hacker/attacker can now spread the virus using the mobile sms, email, mms, gprs, email attachments and various other ways over the internet, thus infecting the systems of other users.

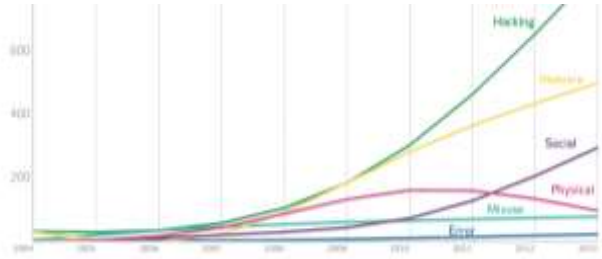

FIG.2 STATISTICAL DATA OF SECURITY BREACHES IN THE SPAN OF YEARS
Source: Associated Newspapers Ltd

C. Statistical Analysis of attacks over internet and mobile communication networks

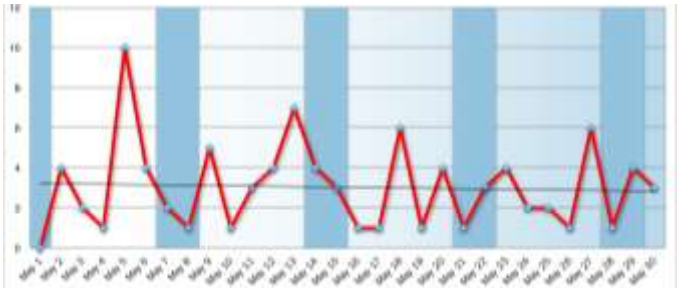

FIG 3. STATISTICAL DATA OF DAILY TRENDS OF ATTACKS IN MAY 2016.
Source: Hackmageddon, Statistic Analysis

The Daily Trend of Attacks graph demonstrates an unmistakable crest amid the principal week (in May 5th) and a level of movement by and large higher amid the primary half. The crests proceed for whatever is left of the month, regardless of the fact that they don't achieve the same level. [6]

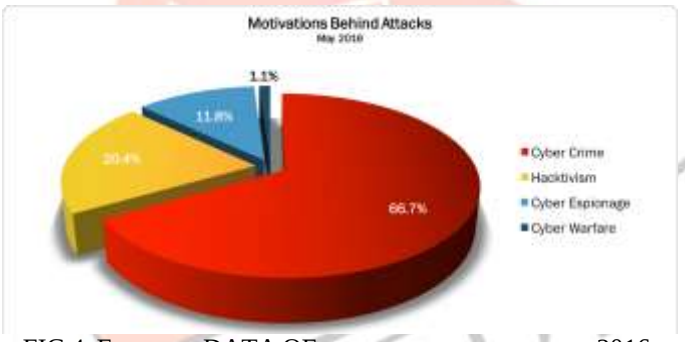

FIG 4. FACTUAL DATA OF ATTACK MOTIVES IN MAY 2016.
Source: Hackmageddon: Statistic Analysis

Digital wrongdoing positions on top of the Motivations Behind Attacks graph with 66.7% (losing about 5 directs looked at toward 71.1% of April). In the same time, Hacktivism is up (from 15.4% of April to 20.4% of May). Digital Espionage develops to 11.8% from 7.2% of April, though Cyberwarfare drops to an unassuming 1.1% (only a solitary occasion). [6]

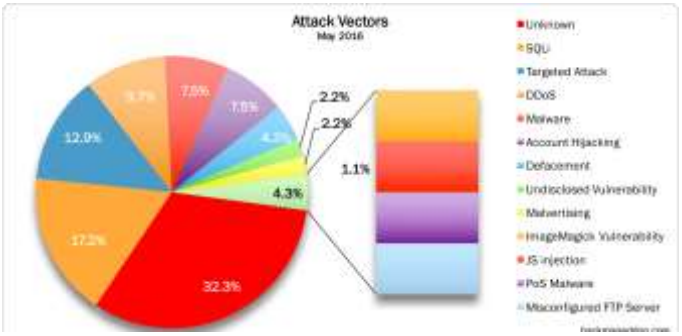

FIG 5. FACTUAL DATA OF DIFFERENT TYPES OF ATTACKS.
Source: Hackmageddon: Statistic Analysis

SQLi positions on top of the known Attack Vectors with 17.2% (with 10.8% in April), in front of focused attacks (12.9% versus 12% in April). Indeed, even for this situation the activities of the Anonymous push DDoS at number three, among the known attacks, with 9.7%, in front of malware and records hijackings, them two with 7.5%.

FIG 6. FACTUAL DATA OF ATTACK MOTIVES IN MAY 2016.
Source: Hackmageddon, Statistic Analysis

Commercial enterprises lead the Distribution of Targets diagram; however, they lose about 10 guides dropping toward 21.5% from 31.3% in April. Money related foundations rank at number two with 15.1%, quickly in front of single people (8.6%). [6]

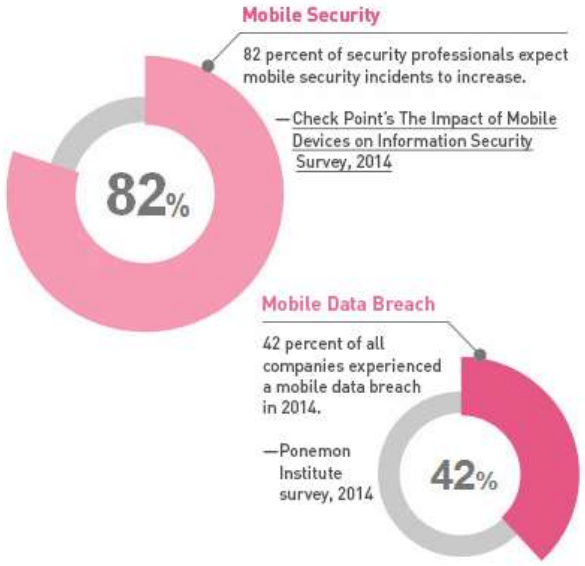

FIG 7. STATISTICAL DATA OF MOBILE SECURITY.
Source: Check Point Software Technology

Versatile innovation has made the system security challenge much greater and more various. Utilization of cell phones and applications has presented an extensive variety of new assault vectors and new information security challenges.

- 27 million strains of malware were made in 2014.
- Advanced mobile dangers can dodge conventional antivirus.
- Document security is restricted on cell phones.
- 42 percent of all organizations encountered a mobile information break in 2014.
- 82 percent of security experts anticipate that mobile security occurrences will increment. [7]

IV. IMPLEMENTATION OF SECURITY

Public-key cryptography is the premise of a few vital security administrations, for example, non-revocation and verification and is a vital component for SSL that is utilized for securing Web correspondence. One public/private key pair is utilized for confirming the authentication of one entity by the other, and common validation requires two key sets. Actually, every entity on the Internet needs a key pair on the off chance that it might be workable for a subjective element to validate some other element. It has hence been anticipated that each player on the Internet will have its own public/private key pair which will shape the premise for the client's or association's computerized personality in electronic situations. This requires the safe generation and circulation of conceivably countless public/private key sets, which represents an impressive key administration challenge.

The Internet get to regularly makes a risk as a security flaw. To shield clients from Internet based attacks and to give satisfactory arrangements when security is forced, cryptographic strategies must be utilized to take care of these issues.

The solution for a wide range of dangers made by criminal exercises ought to depend on cryptographic determination. Verification, message respectability and encryption are imperative incultivating, enhancing, and advancing Internet security. Without such confirmation strategies, an aggressor could mimic anybody and after that access the system. Message uprightness is required in

light of the fact that information might be adjusted as it goes with the Internet. Without confidentiality by encryption, information may end up being truly open. [8]

Various Security Mechanisms below are deployed all together to ensure the safety of Internet and Mobile Communication

A. Cryptographic Algorithms :

Cryptographic Algorithms are implemented in the browsers, applications, wireless networks to provide a security layer for the network. Implementation of these Cryptographic Algorithms ensure the safety of privacy and data of the user.

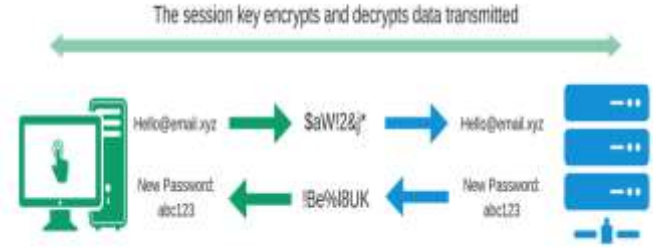

FIG 8. THE PROCESS OF ENCRYPTION.

1) ***Triple Data Encryption Standard(DES)****: Triple DES applies the Data Encryption Standard (DES) figure calculation three times to every information square. The first DES figure's key size of 56 bits was by and large adequate when that calculation was planned, yet the accessibility of expanding computational force made brute-force assaults attainable. Triple DES gives a generally basic strategy for expanding the key size of DES to secure against such attacks, without the need to plan a totally new block cipher algorithm.*

2) ***RSA*** *:* RSA is one of the main handy open key cryptosystems and is generally utilized for secure information transmission. In such a cryptosystem, the encryption key is open and contrasts from the decoding key which is kept mystery. In RSA, this asymmetry depends on the functional trouble of calculating the result of two substantial prime numbers, the factoring issue.

3) ***Blowfish*** *:* Blowfish gives a decent encryption rate in programming and no compelling cryptanalysis of it has been found to date. Be that as it may, the Advanced Encryption Standard (AES) now gets more consideration. This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually.

4) ***Twofish*** *:* Twofish is a symmetric key block cipther with a piece size of 128 bits and key sizes up to 256 bits. It was one of the top five algorithms of the Advanced Encryption Standard challenge, however it was not chose for institutionalization. Twofish is identified with the before block cipher Blowfish .Twofish's unmistakable elements are the utilization of pre-registered key-subordinate S-boxes, and a generally complex key schedule. One portion of a n-bit key is utilized as the genuine encryption key and the other portion of the n-bit key is utilized to adjust the encryption calculation (key-subordinate S-boxes). Twofish gets a few components from different plans; for instance, the pseudo-Hadamard transform (PHT) from the SAFER group of ciphers. Twofish has a structure like DES. Twofish additionally utilizes a Maximum Distance Separable network. Keys used in this algorithm may be up to 256 bits in length and as a symmetric technique, only one key is needed.

5) ***AES****:* The Advanced Encryption Standard (AES) is the algorithm trusted as the excellence by the U.S. Government and various associations. Despite the fact that it is to a great degree proficient in 128-piece structure, AES likewise utilizes keys of 192 and 256 bits for better encryption purposes. AES depends on an outline standard known as a substitution-permutation network, blend of both substitution and permutation, and is quick in both programming and hardware.Unlike its forerunner DES, AES does not utilize a Feistel system. AES is a variation of Rijndael which has an altered block size of 128 bits, and a key size of 128, 192, or 256 bits. By complexity, the Rijndael detail as such is determined with block and key sizes that might be any multiples of 32 bits, both with at least 128 and a greatest of 256 bits.

B. Security functions of the GSM:

The following gives a brief prologue to the security capacities accessible in GSM.

The following functions exist:

1) Access control with the help of a personal smart card (called subscriber identity module, SIM) and PIN (personal identification number).

2) Authentication of the clients towards the system transporter and generation of a session key so as to avert misuse.

3) Communication encryption on the radio network.

4) Concealing the users' identity on the radio network, i.e. a TMSI code is used for the identification of a mobile client instead of the IMSI.[9]

The fundamental security estimations of GSM security can be composed in 4 standards:

1) ***Authentication of a user****:* It gives the ability to mobile entity to demonstrate that it has entry to a specific record with the administrator.

2) ***Ciphering of the data and signaling****:* It requires that all flagging and client information, (for example, instant messages and discourse) are ensured against interceptions by method of ciphering.

3) ***Confidentiality of a user identity****:* It gives IMSI's (International Mobile Subscriber Identity) security. GSM correspondence utilizes IMSI once in a while, it utilizes TMSI (Temporary Mobile Subscriber Identity) to give more secure correspondence and to abstain from unveiling of client's personality. This implies somebody capturing interchanges ought not have the capacity to learn if a specific versatile client is in the zone.

4) ***Using SIM as security module:*** Incase SIM card was taken by adversary, there is still PIN code estimation.[10][11][12][13].

To ensure security in GSM services, the following mechanisms are implemented:

1) ***A3 Algorithm****:* It gives confirmation to the client that it has benefit to get to the framework. The system confirms the endorser using a challenge-response technique.At first the mobile stations is transferred a 128 bit random number over the air.The A3 authentication algorithm receives the RAND number passed through the sim card with the KI.The output of the algorithm is the signed response (SRES) which is transmitted to the mobile station and back to the network again.The AuC present on the the network will compare it's SRES value to the received SRES value.If the two SRES value match the user is authenticated and allowed to join the network [14].

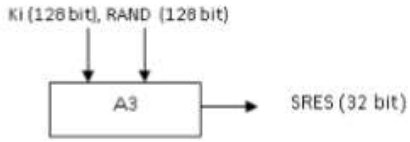

FIG 9. THE A3 ALGORITHM.

2) ***A8 Algorithm****:* A ciphering key is used by GSM to make both client information and the vulnerable air interface secure. After the authorization of the client the RAND from the network and the Ki value alltogether is sent to the A8 ciphering key generation algorithm to produce a new cipher key Kc.The Kc made by the A8 algorithm, is then utilized with the A5 ciphering calculation to encipher or disentangle the information. The A5 calculation is executed in the equipment of the cellular telephone, as it needs to scramble and decode information reporting in real time.[10][14].

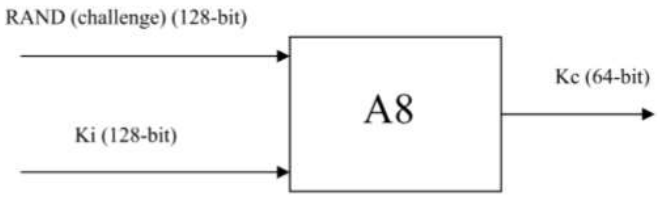

FIG 10. THE A8 ALGORITHM.

3) ***COMP128 Algorithm****:* The COMP128 Algorithm is a hash function which is used to help with the implementation to formerly described A3 and A8 algorithms. While the functioning of the algorithm is to take the RAND and the Ki as an input to the mechanism. The output thus generated is of 128 bit long. Of this 128 bit, the first 32 bits forms the SRES response and the last 54 bits form the sesson key, Kc. The key length now is 54 bits rather than 64 bits, which is the length of the key given as contribution to the A5 calculation. Ten zero-bits are added to the key produced by the COMP128 algorithm . Hence, the key of 64 bits with the last ten bits focused out. This successfully diminishes the key space from 64 bits to 54 bits[15]

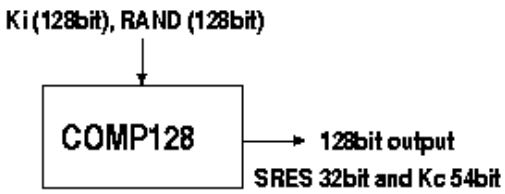

FIG 11. THE COMP128 ALGORITHM

4) ***A5 Algorithm****:* A5 is a stream cipher which can be executed productively on hardware equipment. Different implementations of A5 Algorithm are *:*

i) A5/0
ii) A5/1
iii) A5/2
iv) A5/3 (Used in 3G systems).

The purpose behind the distinctive usage is because of fare limitations of encryption advances. A5/1 is the strongest form and is utilized broadly in the part of Western Europe and America, while the A5/2 is generally utilized in the part of Asia. Nations under UN Sanctions and certain underdeveloped nations utilize the A5/0, which accompanies no encryption. [14] [16]

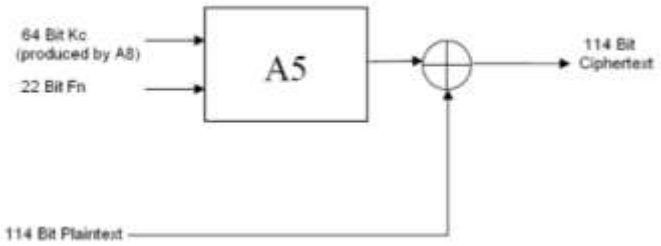

FIG 12. THE A5 ALGORITHM

C. ***Access Control Management***

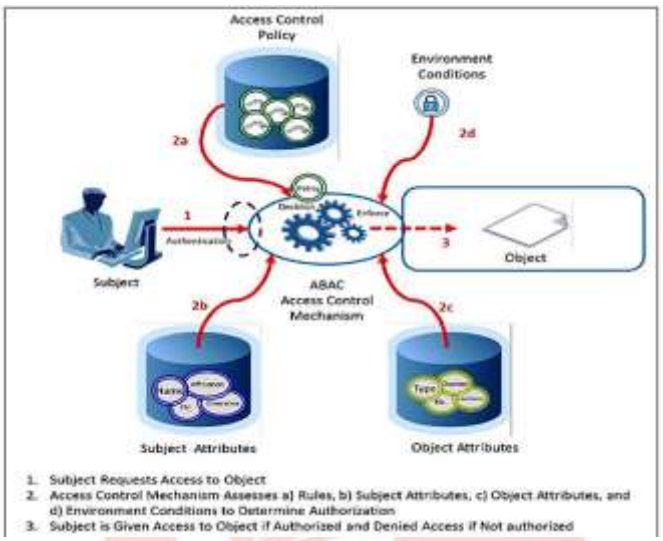

FIG 13. DEMONSTARTION OF WORKING OF ACCESS CONTROL MANAGEMENT.
Source: NIST

Access control management (ACM) frameworks pull together identity, verification and approval to confine what assets a client may get to and in what way that entrance may happen (read, compose, execute, change, and so forth.). ACM arrangements might be founded on various security models, including Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC).

A standard ACM gives an interface through which a client will self-identity, trailed by a system for testing and affirming that identity, and after that a technique for giving rights, or access to data, taking into account the non-repudiation validation of the client. Access control is at the heart of data security and is the crucial reason whereupon the business is based.

The common types of Access control management are:

1) ***Intruder Detection Systems****:* These comprise of interloper cautions and movement indicators that ready you once an interruption is recognized. These frameworks can be fitted within, and also on the outside of your building or office to guarantee that nobody tries to get entrance without your insight.

2) ***Gate Entry Systems****:* A gate entry system allows the monitoring of people in and out of your property. Each individual is provided with appropriate security aspects, as they enter the building. The security aspect will be used to grant the individual the access to specific areas.

3) ***Biometric Readers****:* Biometric identifiers are the particular, quantifiable qualities used to mark and depict individuals. Biometric Identifiers/Readers are classified as:

i) Physiological Characteristics: These illustrations incorporate, however are not restricted to unique mark, palm veins, face acknowledgment, DNA, palm print, hand geometry, iris acknowledgment, retina and smell/fragrance.

ii) Behavioral Characteristics: Behavioral qualities are identified with the example of conduct of a man, including however not restricted to writing, typing rhythm, stride, and voice.

4) ***CCTV Camera Systems***: Video surveillance is essential in high intrigue security regions to give you a recorded visual of individuals movements. CCTV gear might be utilized to watch parts of a procedure from a focal control room, for instance when the entity is not suitable for people. CCTV frameworks may work consistently or just as required to screen a specific occasion. A more propelled type of CCTV, using advanced video recorders (DVRs), gives recording to potentially numerous years, with an assortment of value and execution alternatives and additional elements, (for example, movement recognition and email cautions).

*D. **Firewall** :*

FIG 14. DEMONSTARTION OF WORKING OF FIREWALL.
Source: Microsoft: What is a firewall?

Fundamentally a firewall is a "part or set of entities that confines access between an ensured system and the Internet, or between different arrangements of systems." Firewalls are system security assets that are characterized to control the stream of information between two or more systems. From a high state viewpoint, they can serve as a stifle point, intended to confine, or gag, the stream of system movement, or as a door that performs further handling on the activity past basic gagging limitations**.**
There are distinctive sorts of firewall relying upon where the correspondence is occurring, where the correspondence is blocked and the state that is being followed: [17]

1) ***Network layer or Packet Filters***: They work at a moderately low level of the TCP/IP convention stack, not permitting bundles to go through the firewall unless they coordinate the set up standard set. An administrator may define some standard set of rules; or default tenets may apply.
2) ***Application Layer**:* Application layer firewalls take a shot at the application level of the TCP/IP stack (i.e., all program activity, or all telnet or ftp movement), and may capture all packets setting out to or from an application. They tend to block the leftover packets. On investigating all packets for uncalled material, firewalls can limit or avert the spread of PC worms and Trojans.
3) ***Proxies***: Proxy server may go about as a firewall by reacting to received information packets in the way of an application, while blocking different packets. A customer interfaces with the proxy server, asking for some service, for example, site page, or other asset accessible from an alternate server and the proxy server assesses the solicitation and control its intricacy. Proxies were concocted to add structure and epitome to circulated frameworks
4) ***Network Address Translation***: Firewalls regularly have Network Address Translation (NAT) usefulness, and the hosts ensured behind a firewall generally have addresses in the "private location range". In spite of the fact that NAT all alone is not viewed as a security highlight, concealing the locations of ensured gadgets has turned into a regularly utilized percepted safeguard against system observation.

E. TP method[18]

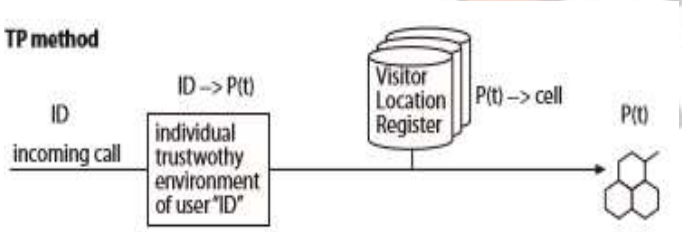

FIG 15. THE WORKING OF TP METHOD IN GSM SERVICE.
Source: Hannes Federrath.

In the TP strategy the locations are no more put away under the ID however under a changing pseudonym P(t). Every change of location is enlisted under another pseudonym, the old one consequently terminates after a specific time.

Since the pseudonym cannot be linked to a call number, not even by the network carrier, no movement profiles can be generated. At the point when an approaching call arrives the system transporter asks for the reliable environment for its present pseudonym, asks for the information bases for the area of the pseudonym P(t) and courses the call to the meeting cell. In the TP strategy cell changes need not be declared to the reliable environment.
The synchronization of the pseudonym is kept on a regular check(i.e. in the scope of minutes to hours). From a specialized perspective, particularly in the dependable environment, this makes issues. It could hinder accessibility, since the client can't be reached to if his dependable zone has crashed or has been straightforwardly attacked.

F. Virtual Private Networks:

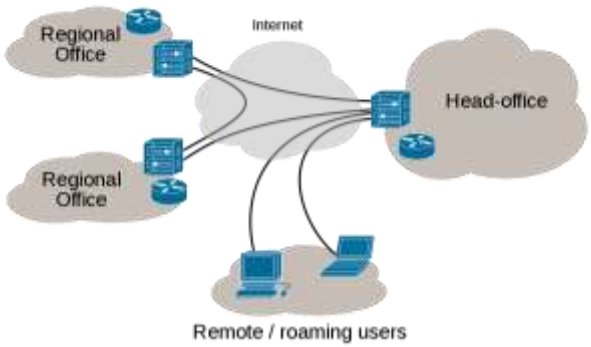

FIG 16. THE WORKING OF VPN.
Source: Wikipedia, VPN

A Virtual Private Network (VPN) is a private correspondences network that makes utilization of open/public systems, as a rule for correspondence between various associations. A VPN is not characteristically secure, however in its most regular incarnation it utilizes encryption to guarantee the classification of information transmitted.
The VPN is frequently seen as a less expensive answer for sending a private system than private rented lines. They regularly serve to secure and guarantee the respectability of correspondence and may likewise ensure the classification of those interchanges while using encryption.
A VPN is made by setting up a virtual point-to-point association using committed associations, virtual tunneling protocols, or activity encryption. A VPN accessible from people in general Internet can give a portion of the advantages of a wide area network (WAN). From a client point of view, the assets accessible inside the private system can be accessed to remotely. [19]

G. Miscellaneous:

Apart from cryptographic algorithms, firewalls and Virtual Private Networks tools like IPSEC, TOR SUITE, BURP SUITE, SQLMAP, ZED ATTACK PROXY, METASPLOIT FRAMEWORK, ARACHNI etc., provide a lot of help in ensuring the safety of Internet, Networks and Mobile Communication.

V. PENETRATION TESTING

A penetration test, or sometimes pentest, is a software attack on a computer system that looks for security weaknesses, potentially gaining access to the computer's features and data.
Penetration Tests are carried out in order to check for the threat vulnerabilities in the internet and mobile communication.

FIG 17. WIDE NUMBER OF TOOLS AVAILABLE IN KALI PENTESTING DISTRIBUTION
Source: Kali Linux, Pentesting Tools.

The goals of Penetration testing are:

1. Identify high-risk vulnerabilities from a combination of lower-risk vulnerabilities exploited in a particular sequence.
2. Identify vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software.
3. Test the ability of network defenders to detect and respond to attacks
4. Provide evidence to support increased investments in security personnel and technology.

Pentesting allows a user or an enterprise to ensure the safety of its services so as to maintain their privacy on the web. [20] [21]

VI. CONCLUSION

Security is the most basic and essential requirement for today's users. A single security policy cannot help with the
Safety of information, personal data and credentials online.
It is crucial to implement different types of strategies combined together to form a solid security layer.
Cryptographic algorithms provide a concrete layer over application networks. Keys in communication must be verified at every instance of time so as to ensure no intrusion in the network. Firewall and Antivirus keep a check over unknown programs by continuously checking the virus definitions.
VPN's, IPSEC, BURP SUITE and various other tools provide a helping hand for determining the security level of networks and mobile communication.

Penetration Testing, however, may not be usable by common people but provide a concrete reliability for ensuring the security levels of the systems in the administration. Today a user cannot be 100% safe online, but we can up to a certain extent make sure that we do as much as we can to stay safe.

REFERENCES

[1] PandaLabs: Quarterly Report PandaLabs, January-March 2011
[2] Symantec: Symantec Report Finds Cyber Threats Skyrocket in Volume and Sophistication.
[3] National Institute of Standards and Technology: Guidelines on Cell Phone and PDA Security.
[4] Trend Micro: Smartphone Users: Not Smart Enough About Security.
[5] Google Images www.google.com
[6] Hackmegaddon.com: May 2016 Cyber Attack Statistics
[7] Check point software Technologies
[8] Security in Mobile Communications: Challenges and Opportunities
Authors : Audun Jøsang Gunnar Sanderud
[9] Man in the middle attack, University of Bern.
[10] Ammar Yasir Korkusuz: Security in GSM Networks.
[11] Helsinki University of Technology, GSM Security, Mikko Suominen, 2003.
[12] A Contemporary Foreword on GSM Security, Paulo S. Pagliusi
[13] Security in the GSM system, Jeremy Quirke, 2004
[14] The GSM Standard, SANS Institute, 2001
[15] Can you clone a GSM Smart Card (SIM)?, Charles Brookson, 2002
[16] GSM Security Overview, Gregory Greenman
[17] Wikipedia : Firewall Systems
[18] Hannes Federrath: Protection in Mobile Communications Edition: 1999
[19] Microsoft Technect: Virtual Private Networking.
[20] Kali Linux Pentesting Linux Distribution
[21] Wikipedia: Pentesting