iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** I **Month of publication:** January 2022

DOI: https://doi.org/10.22214/ijraset.2022.39843

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: 7.538
Volume 10 Issue I Jan 2022- Available at www.ijraset.com

Cyber Security Frameworks

Arunabh Singh[1], Suraj Kumar Singh[2], Ayush Soni[3], Krishna Gullapalli[4], Vimlesh Singh[5]
[1, 2, 3, 4, 5]*Electronics and Communications Department, Manav Rachna International Institute of Research and Studies*

Abstract: ***In this paper we attempt to explain and establish certain frameworks that can be assessed for implementing security systems against cyber-threats and cyber-criminals. We give a brief overview of electronic signature generation procedures which include its validation and efficiency for promoting cyber security for confidential documents and information stored in the cloud. We strictly avoid the mathematical modelling of the electronic signature generation process as it is beyond the scope of this paper, instead we take a theoretical approach to explain the procedures.***
We also model the threats posed by a malicious hacker seeking to induce disturbances in the functioning of a power transmission grid via the means of cyber-physical networks and systems. We use the strategy of a load redistribution attack, while clearly acknowledging that the hacker would form its decision policy on inadequate information.
Our research indicate that inaccurate admittance values often cause moderately invasive cyber-attacks that still compromise the grid security, while inadequate capacity values result in comparatively less efficient attacks. In the end we propose a security framework for the security systems utilised by companies and corporations at global scale to conduct cyber-security related operations.
Keywords: Electronic signature, Key pair, sequence modelling, hacker, power transmission grid, Threat response, framework.

I. INTRODUCTION

An electronic signature is a digital analogue of a written signature. A valid electronic signature, where the prerequisites are satisfied, gives a recipient very strong reason to believe that the message was created by a known sender, and that the message was not altered in transit. Electronic signatures are a standard element of most cryptographic protocol suites, and are commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering. electronic signatures employ asymmetric cryptography. In many instances, they provide a layer of validation and security to messages sent through a non-secure channel: Properly implemented, an electronic signature gives the receiver reason to believe the message was sent by the claimed sender. Electronic signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Electronic signature schemes, in the sense used here, are cryptographically based, and must be implemented properly to be effective. They can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming his private key remains secret. Further, some non-repudiation schemes offer a timestamp for the digital signature, so that even if the private key is exposed, the signature is valid. Electronically signed messages may be anything representable as a bitstring: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol. digital signature scheme typically consists of three algorithms;

1) A *key generation* algorithm that selects a *private key* uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding *public key*.
2) A *signing* algorithm that, given a message and a private key, produces a signature.
3) A *signature verifying* algorithm that, given the message, public key and signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key.
In the second topic we focus on cyber-physical risk modelling while obviously acknowledging that a hacker would probably base his strategy on imperfect information. Indeed, the ability of transmission branches to safely withstand loading depends upon ambient conditions and the tolerance of grid-operatives for greater loading levels when these ambient conditions are beneficial. To perform our investigation we use the Monte Carlo framework while modelling sequentially the decisions of a flawed hacker, the corresponding reaction of the grid-operative and finally the resultant state of the grid.

©IJRASET: All Rights are Reserved

In addition to the basic limitations included in the recent developments of such models, we enact unusual constraint expressions to reflect a malicious hacker with the purpose of inducing a challenging and vulnerable state so as to trigger a potentially cascading failure event. Our analysis showcases that informational imperfections imply a broad spectrum of potential cyber-attacks and of respective physical impacts on the system.

Moreover, the spectrum of potential cyber-attacks clearly features groups of common attacked assets in the cyber sub-system and common affected assets in the physical sub-system. The implication is that protecting the cyber sub-system to prevent and detect intrusion of such common attacked assets and/or the physical sub-system to withstand the possible failure of such common affected assets could be effective cyber-physical risk management strategies.

We model a malicious cyber-attacker seeking to maximize the grid physical insecurity through a load redistribution attack. More specifically, we consider an attacker falsifying bus load measurements so as to mislead the grid-operator into perceiving the grid as insecure and implementing unnecessarily generation redispatch actions.

The hacker's aim is to augment the total extent of branch overloads caused by the introduction of false measurements and the resulting re-dispatching of the misinformed grid-operative.

In the third topic we discuss the effective models of frameworks we have designed so as to be utilised by the organizations to resist the security breaches that occur in their sub systems. The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program for the management of risk—that is, the risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation of information systems. Risk-based approaches to security control selection and specification consider effectiveness, efficiency, and constraints due to applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines. To integrate the risk management process throughout the organization and more effectively address mission/business concerns, a three-stage approach is employed that addresses risk at the:

a) organization
b) business process
c) information system

The risk management process is carried out across the three stages with the global objective of continuous improvement in the organization's risk-related activities and effective inter-tier and intra-tier communication among all proprietors having a shared interest in the success of the organization. Stage-1 provides a prioritization of organizational missions and their functions which in turn leads to investment strategies and funding decisions i.e. supporting cost-effective, efficient information technology solutions consistent with the strategic goals and objectives of the organization and measures of performance. Stage-2 andSstage-3includes:

- Defining the business procedures required to support the organizational functions
- Determining the security categories of the information systems needed to execute the mission/business processes.
- Incorporating information security requirements into the business processes.
- Establishing an enterprise architecture to ease the distribution of security controls to organizational information systems and the environments in which those systems operate.

II. ELECTRONIC SIGNATURE

A electronic signature is represented in a computer as a collection of bits. An electronic signature is processed using a set of rules and a set of parameters that allow the identity of the signatory and the integrity of the data to be verified. Electronic signatures may be created on storage as well as transmission data. Signature creation uses a private key to generate an electronic signature and signature verifier uses the public key that corresponds to it. Each signatory(proprietor) possesses a personal/non-public and public key pair. Public keys may be known by the public while the non-public keys are kept secret. Anyone can verify the signature by utilizing the signatory's public key. Only the proprietor that possesses the non-public key can perform signature creation. A hash characteristic is used in the signature creation process to obtain a compressed form of the documents to be signed. The compressed version of the documents is known as data inventory.

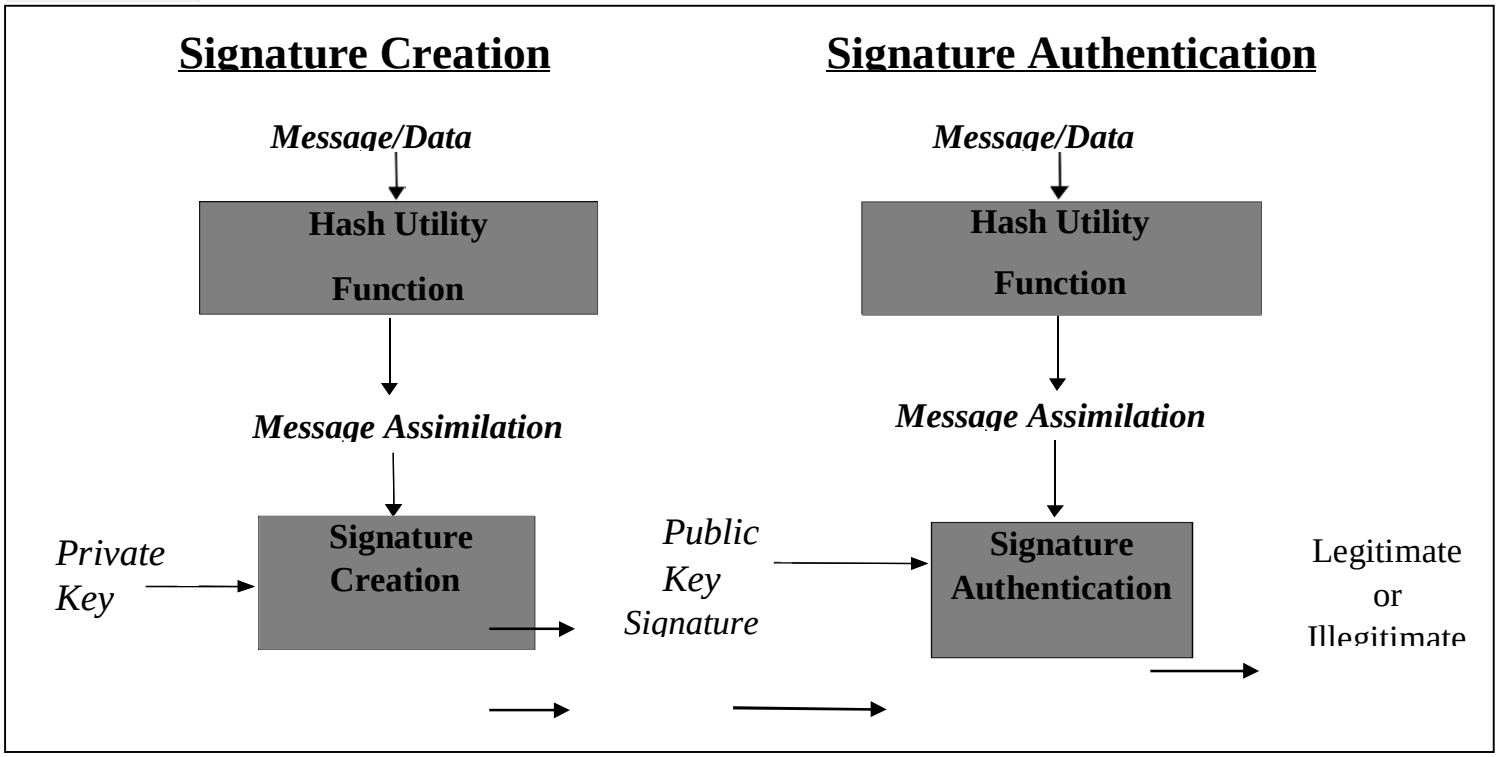


Figure :1 Electronic signature procedures

The data inventory acts as the input to the electronic signature computation to create the signature. A electronic signature is an digital equivalent of a written signature. The electronic signature can be utilised to provide guarantee that the alleged signatory has signed the documents. In addition, an electronic signature may be utilised to confirm if the documents were altered after they were signed or not. These guarantees can be attained irrespective of whether the information was obtained in a transmission or from storage. An electronic signature algorithm includes a signature creation and a signature verification procedure. A signatory(proprietor) utilises the generation procedure to create an electronic signature based on the given records while the verifier verifies the validity of the signature. All signatories have a public and non-public key and they are the sole possessor of that key pair. As shown in Figure 1, the non-public key is utilised in the signature creation process. The key pair possessor is the only entity that is permitted to use the non-public key to create electronic signatures. For the purpose of preventing other beings from claiming to be the key pair possessor and using the non-public key to create illegal signatures, the non-public key should remain confidential and encrypted. The accepted electronic signature algorithms are devised to thwart an enemy who lacks the knowledge about the proprietor's private key from forging the exact signature of the proprietor on a different document. In other words, signatures are designed so that they cannot be forged. The public key might not be kept confidential, but its veracity must be preserved. Everyone can confirm a perfectly signed document by making use of the public key. For both the signature creation and verification procedures, the document (i.e., the signed records) is transformed into a fixed-duration representation of the document with the help of an authorized hash characteristic. Both the original document and the electronic signature must be made accessible to a verifier. A verifier needs guarantee that the public key to be utilised to verify a signature belongs to the person that alleges to have created the computerised signature. That is, a verifier needs guarantee that the proprietor is the genuine owner of the public and non-public key pair used to create computerised signature. A binding of the proprietor's identification and his public key should be put into effect to provide this guarantee. A verifier also needs guarantee that the key pair possessor actually owns the non-public key coupled with the public key, and that the non- public key is mathematically accurate . By attaining these guarantees, the verifier has affirmation that if the electronic signature is perfectly verified by the usage of the public key, the electronic signature is legitimate. Electronic signature authentication includes the mathematical authentication of the signature and also the suitable guarantees. The following reasons give an explanation as to why such guarantees are necessary.

1) If a verifier does not acquire guarantee that a proprietor is the genuine possessor of the key pair whose public key is used to verify a signature, the issue of duplicating a signature is decreased to the issue of wrongly claiming another person's identity.

2) If the public key which is used to verify a signature is mathematically invalid, the claims used to determine the cryptographic power of the signature algorithm will not be applicable.

3) If the public key set-up is unable to provide guarantee to the verifier that the possessor of a key pair has confirmed of having the required knowledge of a non-public/personal key that corresponds to the possessor's public key, then it might be probable for an dishonest entity to have their identity bound to the key pair which is utilised by some other person. The deceitful entity might then claim to be the signatory that has signed the confidential documents by using that key pair.

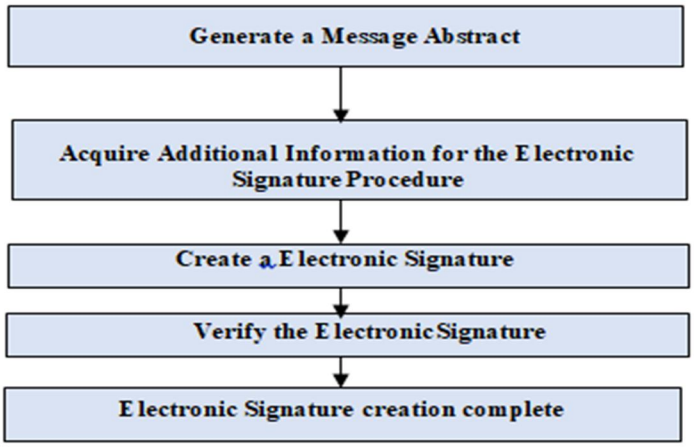


Figure-2 Electronic Signature generation

Figure 2 depicts the steps that are performed by an intended signatory (i.e., the entity that generates a digital signature). Prior to the generation of a digital signature, a message digest shall be generated on the information to be signed using an appropriate approved hash characteristic. Utilizing the chosen electronic signature algorithm, the non-public key, the data inventory, and all the other information necessary for the electronic signature procedure, a computerised signature will be created in accordance with requirements of the proprietor. The signatory may additionally verify the electronic signature using the verification procedure and the corresponding public key. This additional verification aids in the last check to detect (if any) hidden signature computation faults.

III. SEQUENCE MODELLING

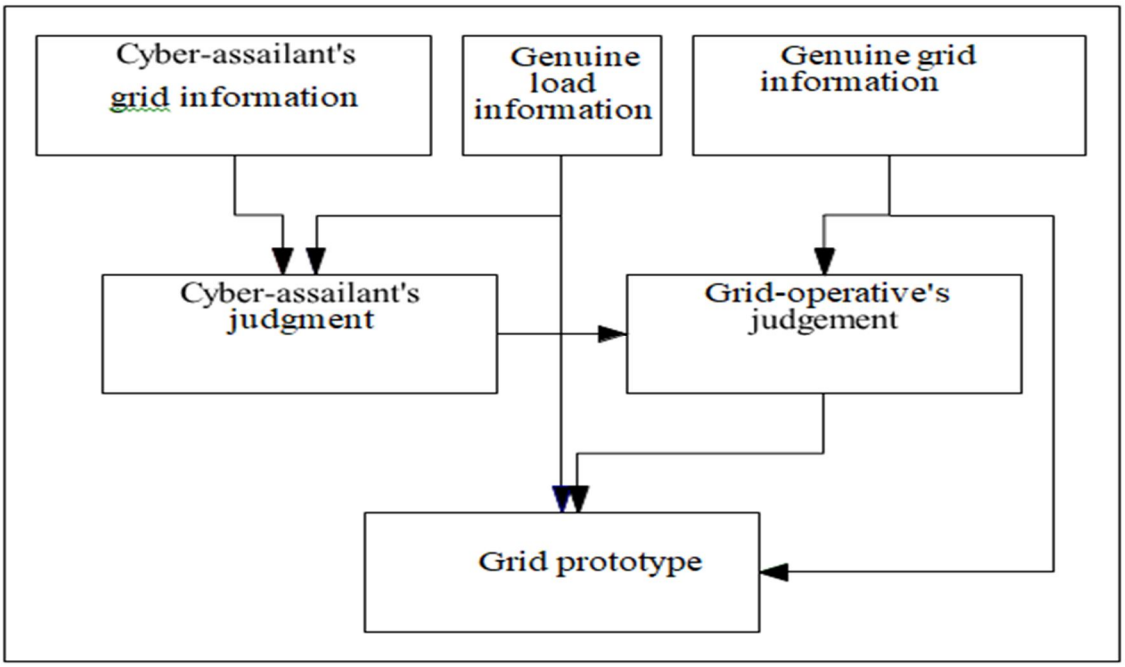


Figure-3 Inadequate information modelling

Fig. 3 presents the proposed flowchart for modelling a cyber-attack with inadequate data. At the top layer of this figure we distinguish between two different datasets for the grid, the "hacker's" and "genuine" grid data. The former includes the data on the networking grid that a hacker would exploit to decide his hacking strategy. The latter includes the accurate values for all the parameters of the grid and is only accessible to the grid-operative.

The load data is not included in any of these two datasets as it is predicted to be a "genuine" set of data only known to the hacker. The middle layer of Fig. 3 represents the contact between the hacker and the grid-operative by means of two distinctive decision-making models, which are solved sequentially.

First, the box "hacker's decision-making" corresponds to bilevel model, used by the hacker to identify his attack vector for load redistribution. The box "grid-operative's decision-making" models the reaction of the grid-operative to the attack. We must stress here that, even though a model for the grid-operative's reaction is embedded in the hacker's problem, the true reaction of the grid-operative to the attack vector will be based on the true grid data he has access to. The lower layer of Fig. 3 illustrates a model of the physical impact of the attack on the grid.

We should also acknowledge that restricting the physical models and equations in the grid- operative's decision-making model to match those of the hacker is not necessary by default. We made such choice here so as to isolate the impact of inaccurate data, and refer the reader to for a study of the impact of simplifications in the hacker's modelling of a grid-operative's decision-making. which is solved by combining:

1) The genuine load information
2) The genuine grid information
3) The re-distribution decisions the grid-operative would take given the load redistribution attack and his understanding of genuine grid information.

Seeking to isolate the effect of imperfect information, in our implementation we combine such inputs through the same physical model as in the hacker's decision-making problem to measure grid insecurity in terms of the number and magnitude of overloaded branches.

Cyber-physical risk assessment serves to quantify the threat posed by a malicious hacker. The concept of the correct information network-attack is commonly utilized in assessment applications, to foresee the worst-case impact on the system. Acknowledging a hacker's incorrect information yields a set of random attack samples and respective impact statistics. Beyond the expected value and distribution of the impact statistics over the Monte Carlo samples, we propose to examine the risk of an attack with inadequate data by means of the following exclusive categories.

a) *Ideal*: all samples wherein the attack vector of an inefficient attack matches the vector from the correct information network-attack.
b) *Victory*: all other samples wherein an inefficient attack would still achieve the hacker's goals in terms of minimum number of overloaded branches with a flow above the respective threshold.
c) *Partial victory*: all other samples where an inefficient attack results in overloading at least one transmission branch with a flow above the respective threshold.
d) *Failure*: all samples wherein an inefficient attack would cause no branch overload.
e) *No effort*: all samples wherein the hacker, given his inadequate information, fails to identify a feasible attack on the networking grid.

The share of samples in the first category shows the relevance of the worst-case perfect information cyber-attack, or alternatively the relevance of acknowledging a hacker's informational imperfections.

Note that this category does not only include instances wherein the hacker's grid data randomly turn out to be perfectly accurate, but also instances where the hacker's informational imperfections have no effect on his strategy. A larger share of samples in the last two categories indicates that the cyber-physical system is fundamentally more secure, either by "absorbing" the physical impact of imperfect attacks or by way of appearing more vigorous to the hacker. We further assess the risk posed by the flawed hacker by means of the categories introduced through the Fig. 4.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue I Jan 2022- Available at www.ijraset.com

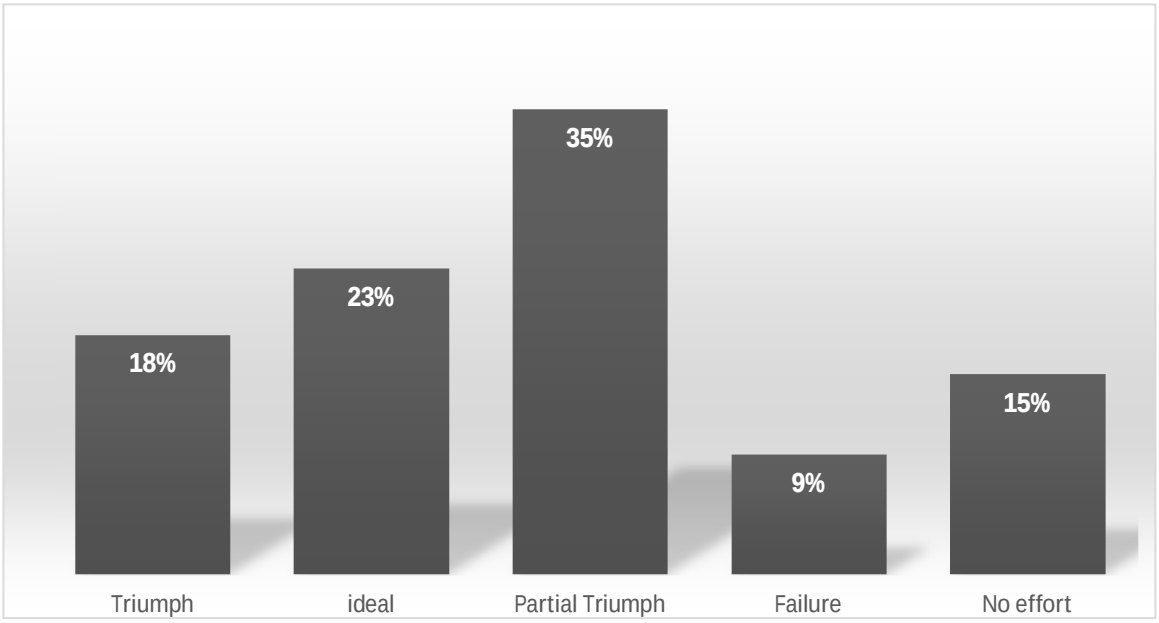


Figure-4 Classification of attacks based on inadequate admittance information

As shown in this chart, due to the assumed informational imperfections the hacker would only be able to correctly identify the optimal perfect information attack vector from Fig. 3 on 23.% of the simulated instances. Conversely, on 15% of the sampled instances the hacker would falsely believe that it would be fruitless to launch any load redistribution attack while on 9% of the instances, he would launch an attack that would not be harmful to the grid. Observing that on 35% of the instances an attack with imperfect information would cause an overflow on at least two grid branches. While continuing the analysis by henceforth considering the case where the hacker relies on inaccurate data about the branch capabilities only. We sampled furthermore 10000 grids with erroneous load data, by introducing a unique error term to the capability value of each and every branch, which was evenly distributed in the range ±5%. With such notions, the average cyber-attack impact reduces to 24.3 MW while the number of unique cyber-attacks increases to 6000.

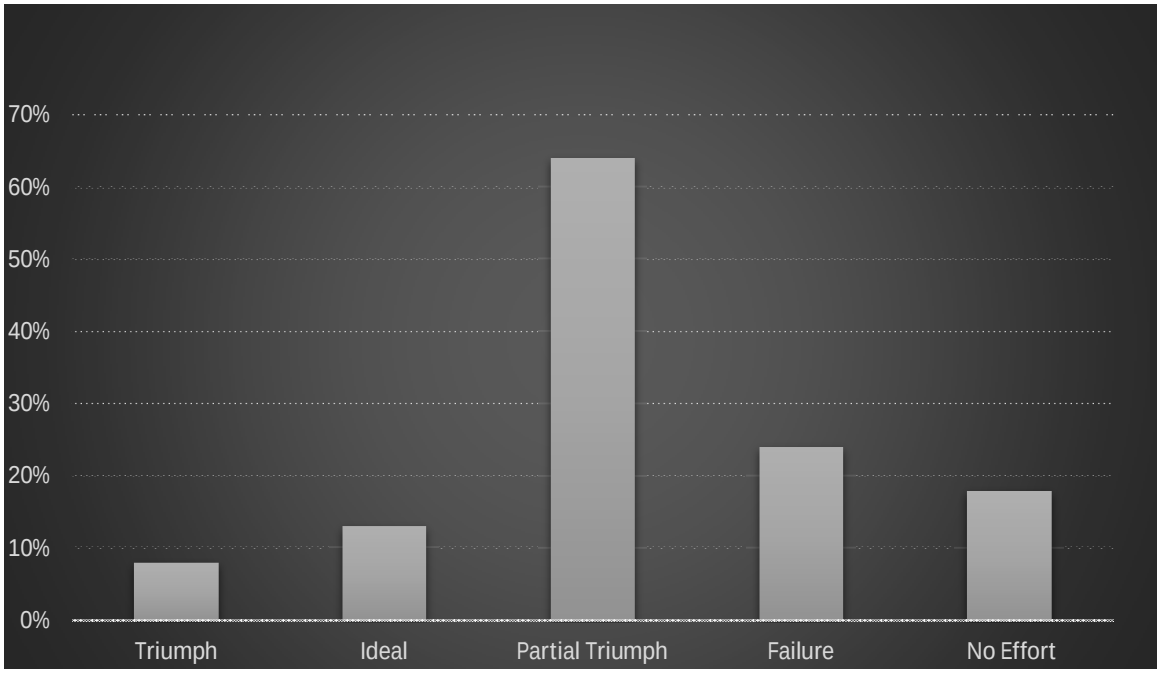


Figure-5 Classification based on inadequate branch capabilities information

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Fig. 5 presents the classification of the random attacks as in accordance with the categories introduced above. The qualitative difference corresponding to flawed admittance values is striking in comparison to Fig. 4. Indeed, for the same error range:

- The proportion of ideal attacks has collapsed.
- The proportion of completely successful attacks is halved.
- The proportion of partially successful attacks is significantly increased.
- The proportion of unsuccessful attacks is comparatively increased.

In other words, inadequate data about branch capabilities leads to less efficient cyber-attacks posing a smaller risk to the system cyber security. We can identify systematic reasons for this finding. Indeed, in case the cyber- attacker undermines branch capabilities, he is disposed to overestimating the effect of an attack vector for:

- The grid-operative to redispatch generation to avoid overloads under the load redistribution
- Causing actual overloads by way of the erroneous redispatch.

IV. THREAT RESPONSE FRAMEWORK

We have conducted a survey based on the cyber-security issues(threats) faced by corporations and institutions which deals with information technologies and data communication. The threats and their underlying causes are addressed in the following table(Fig - 6)

Types of Threats	Causes
Unauthorized Data transmission	i) Data leakage ii) Screen scrapping iii) Backup losses iv) Email and social media
Data corruption	i) Modification by other applications ii) Undetected interference iii) Pirated devices
Data loss	i) Lost device ii) Unsanctioned physical access
Malware	i) PN-OS alteration ii) Application alteration iii) Virus

Figure -6 Threats faced by organizations at global scale

In order to devise certain defensive mechanisms to detect and resolve these issues we have created a Threat Response Frameworks(TRF) whose primary goal is to address these issues and take appropriate measures, accordingly, as depicted in Figure 7. This flowchart focuses on the step by step procedure of the TRF. The TRF addresses the security concerns of organizations related to the design, development, implementation, operation, and disposal of information systems and the environments in which those systems operate. The TRF consists of the following six stages:

1) Classify the communication networking system.
2) Choose the appropriate safety control mechanisms centred on the outcomes of the security classification and put into effect the tailoring assistance.
3) Execute the safety control mechanisms and document the layout, progress, and execution details.
4) Evaluate the security control mechanisms to ascertain the extent to which the controls are executed accurately, functioning as intended, and generating the desired results.
5) Permit communication system administration based on the determination of threats to organizational administration.
6) Supervise the security mechanisms in the communication systems and their networks of operation on a continuous basis to ascertain control efficiency.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue I Jan 2022- Available at www.ijraset.com

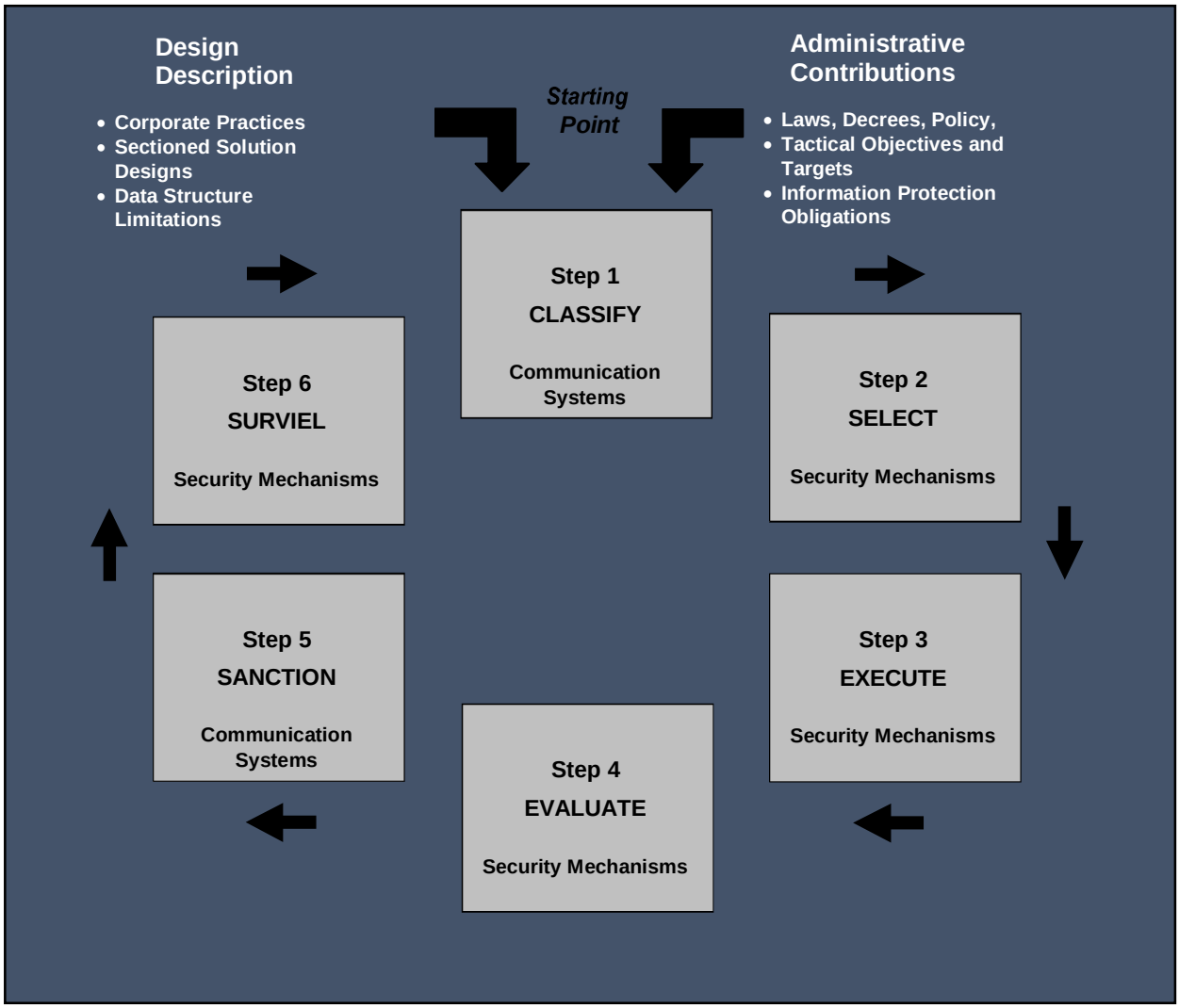


Figure-7 Threat Response Framework(TRF)

Organizational level analysis of threats, which includes the use of specified and reliable threat evidence, vulnerability evidence, and the possibility of these threats abusing liabilities to cause adverse damage, lead and advise the tailoring procedure and the last selection of security mechanisms. The decisive and mutually acceptable set of security mechanisms referring to specified administrative and business needs and forbearance for threat is documented with suitable reasoning in the safety models for the communication networks and devices. Attaining adequate data for organizations, business procedures and communication networks is a comprehensive responsibility which demands:

a) Clearly formulated cyber security obligations and provisions.
b) Well-designed and sturdy communication networking devices based on appropriate hardware, firmware, and software development procedures.
c) Cyber-Security engineering principles to efficiently integrate information technology systems into organizational information systems.
d) Cyber-Security practices should be well documented and effortlessly integrated with the guidance constraints and regular schedules of organizational staff with security assignments.
e) Continuous monitoring of organizational communication networks to determine the ongoing effectiveness of deployed security controls, changes in systems and environments of operation, and compliance with legislation, directives, policies, and standards.
f) Life cycle management of security planning and system improvement.

©IJRASET: All Rights are Reserved

V. CONCLUSION

We discussed the advantages and the design procedures of an electronic signature , we also discussed the significance of key pairs along with the functions of public and non-public key. From our analysis it is clear that though the signature generation and verification process is tedious, but the efficiency of the electronic signature in protecting the confidential data stored in the cloud and preventing the forgery of the signature by cyber-criminals is outstanding. We also conducted a case study about the sequence modelling of a power transmission grid with inadequate admittance and branch data. From a risk assessment viewpoint, we have found in our case study that inaccurate knowledge of the grid admittance matrix is not a significant inhibition to inducing physical insecurity through the cyber sub-system. On the other hand, relying on inadequate information on the branch transmission capabilities was found to lead to a much stronger reduction of the risk as it might lead a hacker to either:

i) Launch less effective attacks while miscalculating some branch capabilities.

ii) Give up the idea of attacking the system when overemphasizing the branch capabilities.

From a risk management perspective, we most remarkably observed in our case study that in spite of random inaccuracies, 90% of the random attack vectors would target at minimum one branch in common with the “perfect” information attack. This implies that supervising the functioning of the branches for a perfectly informed hacker i.e., the “worst-case” from the perspective of the power transmission grid end-users, would prove to be a very efficient detection strategy. After this we proposed a framework of our own making for establishing the security systems at organizational or global level, which can improve operational efficiencies to a great extent, else they are exposed to potentially new attack surfaces and security liabilities if not properly protected from Cyber intrusion. Each and every machine joins “a system of systems” as it gets interlinked with more and more devices. Technological developments like 5G will most likely boost the usage of the security mechanisms and models which would in turn require the appropriate frameworks for their implementation and execution. Practically, anything and everything is at the risk of becoming vulnerable i.e. from valuable assets or services, crucial projects and tasks assigned in the cloud, process controlling subsystems in cyber-physical systems to confidential business and operational data. There two major approach for management of cyber-threats in a system:

1) Qualiative Approach
2) Quantitative approaches

For instance, if an electronics manufacturer uses Safety Instrumented System (SIS) controllers to analyze data from industrial equipment systems so as to provide aid to the management and functioning of machineries. Iterations to these systems may cause physical damage and interrupt operations. Electronics manufacturers are at high risk of exposing automated equipment and computerized processes to adverse Cyber-attacks and their consequences this come in qualitative approach. Four layer cyber security management system is one of technique which provide effective solution to risk management in a cyber-physical system. A four layer system consist of

a) Ecosystem
b) Infrastructure
c) Performance

When this data is assessed, it provides companies and organizations a clear understanding of their manufacturing procedures and creates several new business and production opportunities. Organizations thus require certain resources which will contribute in protecting their assets and networks, along with their whole information ecosystems. Perfected Security frameworks and system models thus became inevitable so as to strengthen or substitute human interference in the recognition and restriction of cyber security threats or breaches. Such models rely upon artificial intelligence(AI), machine learning, business analytics and instrumentation.

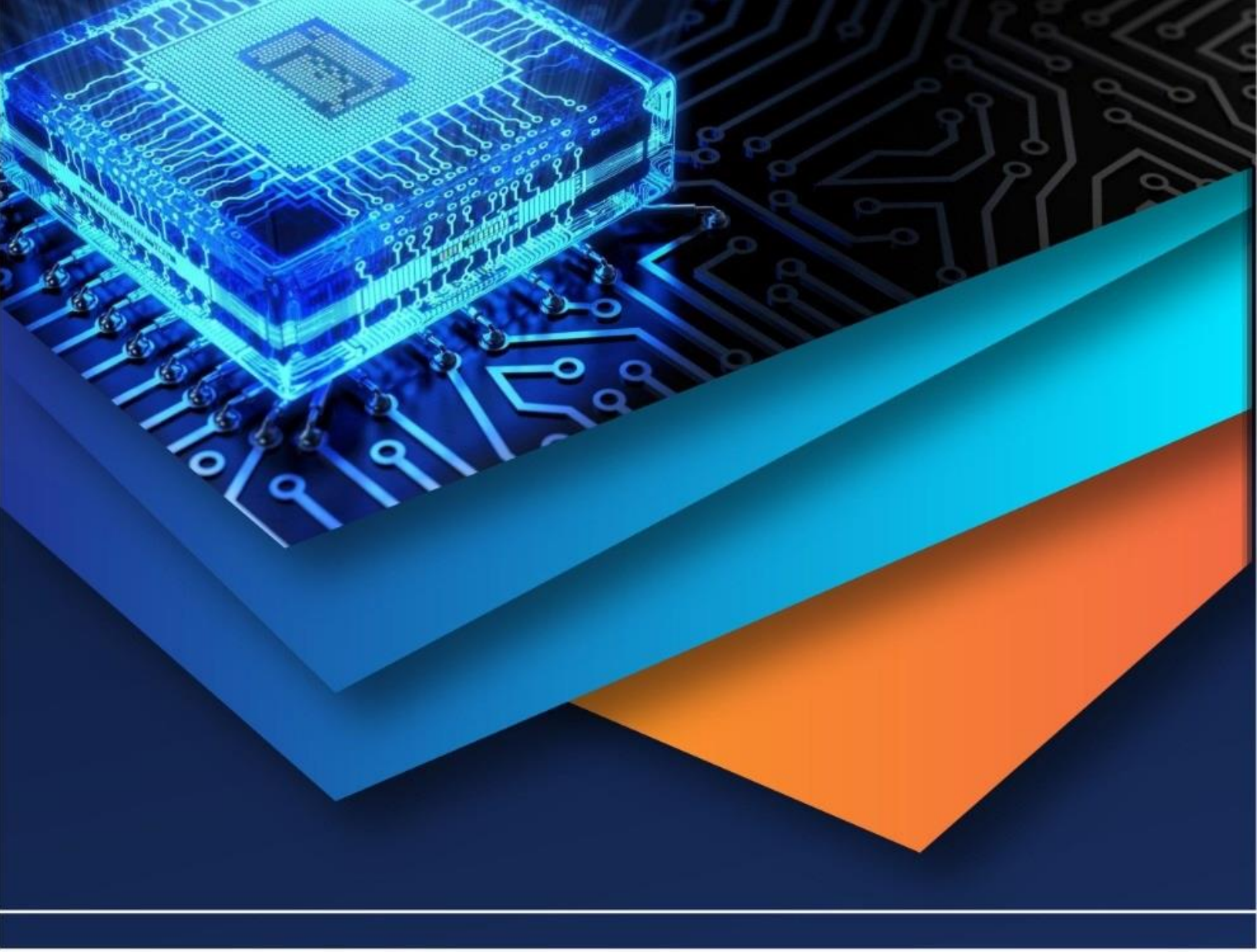
REFERENCES

[1] Damgard, P. Landrock, and C. Pomerance, C. “Average Case Error Estimates for the Strong Probable Prime Test,” Mathematics of Computation, v. 61, No, 203, pp. 177-194, 1993.
[2] A.J Menezes, P.C. Oorschot, and S.A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996.
[3] H.C. Williams. “A p+1 Method of factoring”. Math. Comp. 39, 225-234, 1982.
[4] D.E. Knuth, The Art of Computer Programming, Vol. 2, 3rd Ed., Addison-Wesley, 1998, Algorithm P, page 395.
[5] R. Baillie and S.S. Wagstaff Jr., Mathematics of Computation, V. 35 (1980), pages 1391 – 1417
[6] D. Kirschen and F. Bouffard, “Keeping the lights on and the information flowing,” IEEE Power and Energy Magazine, vol. 7, no. 1, pp. 50–60, 2009.
[7] H. Zhang, B. Liu, and H. Wu, “Smart grid cyber-physical attack and defence: A review,” IEEE Access, vol. 9, pp. 29 641–29 659, 2021.
[8] H. He and J. Yan, “Cyber-physical attacks and defences in the smart grid: a survey,” IET Cyber-Physical Systems: Theory & Applications, vol. 1, pp. 13–27(14), December 2016. [Online]. Available: https: //digital-library.theiet.org/content/journals/10.1049/iet-cps.2016.0019

©IJRASET: All Rights are Reserved

[9] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," vol. 14, no. 1, Jun. 2011. [Online]. Available: https://doi.org/10.1145/1952982.1952995
[10] Y. Yuan, Z. Li, and K. Ren, "Modelling load redistribution attacks in power systems," IEEE Transactions on Smart Grid, vol. 2, no. 2, pp.382–390, 2011.
[11] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," IEEE Transactions on Power Systems, vol. 31, no. 5, pp. 3864–3872, 2015.
[12] J. Zhang and L. Sankar, "Physical system consequences of unobservable state-and-topology cyber-physical attacks," IEEE Transactions on Smart Grid, vol. 7, no. 4, 2016.
[13] M. Tian, M. Cui, Z. Dong, X. Wang, S. Yin, and L. Zhao, "Multilevel programming-based coordinated cyber physical attacks and countermeasures in smart grid," IEEE Access, vol. 7, pp. 9836–9847, 2019.
[14] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in 2012 IEEE Global Communications Conference (GLOBECOM), 2012, pp. 3153–3158.
[15] J. Zhang, Z. Chu, L. Sankar, and O. Kosut, "Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems?" IEEE Transactions on Power Systems, vol. 33, no. 5, pp. 4775–4786, 2018.
[16] National Institute of Standards and Technology Special Publication 800-25, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication, October 2000.
[17] National Institute of Standards and Technology Special Publication 800-27, Revision A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2004.
[18] National Institute of Standards and Technology Special Publication 800-28, Version 2, Guidelines on Active Content and Mobile Code, March 2008.
[19] National Institute of Standards and Technology Special Publication 800-29, A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2, June 2001.
[20] National Institute of Standards and Technology Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments, September 2012.
[21] National Institute of Standards and Technology Special Publication 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure, February 2001.
[22] National Institute of Standards and Technology Special Publication 800-33, Underlying Technical Models for Information Technology Security, December 2001.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)