International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

A Doctrinal Approach to Information Security

Tummala Bindu Madhavi[1], M. Anitha[2], T.VijayaSree[3], S.Harika[4]
[1, 2, 3,4]*Assistant Professor, S.R.K.Institute of Technology, Enikapadu, Vijayawada*

Abstract*: "Security" it is the most common word used by all the sectors of the world. This word encapsulates various features because it is the most essential word used to develop any sort of applications in the form of technology .As technology is upgrading its nature its nature also getting changed because a technology up gradation or integration leads to the change of each and every sector. Because technology is not confined to an individual its a progressive establishment of various sectors. The most recent trends in the technology up gradation are IOT, CLOUD, ARTIFICIAL INTELLIGENCE and BIOINFORMATICS. This paper is a small demonstration of adding the security modes in these aspects because in order to open a door a key is essential and this paper represents the key aspects.

Keywords*: Doctrinal, Encapsulate, Elucidate, Elaborate,"We" represents the 4 authors.

I. INTRODUCTION

Let us first elaborately see the current definition of the paper "Doctrinal" is nothing but a philosophical way of studying a subject and attaining the knowledge of that subject. Security is the most important aspect that is concerning and governing all the fields now days.

In our daily life we need to security when we use a mobile device we require security when we use a bike or a car we require security. This security was provided in the form of a hardware component or as a software component when we take this as an industrial approach.

The motive behind saying the term doctrinal is that the width and depth of this particular subject or term security must be elaborated to enhance the standard world definition.

Security or security related aspects must be understood to a lay man because how far we go doesn't matter much than how far the technology reached a common lay man that is the key security issue. Because a security must be provided to a lay man in a secured way. With insecurity approach to a secured approach a lay man must identify the need of it. And make this authoritative term to reach a lay man in the form of a physical approach or a software approach or a collaborative approach.

Before we go through these aspects let us see the definition of information security

A. Definitions Of Information Security

Information security (infosec) is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Infosec responsibilities include establishing a set of business processes that will protect information assets regardless of how the information is formatted or whether it is in transit, is being processed or is at rest in storage.

Information security (IS) is designed to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions. Confidentiality, integrity and availability are sometimes referred to as the CIA Triad of information security. This triad has evolved into what is commonly termed the Parkerian hexad, which includes confidentiality, possession (or control), integrity, authenticity, availability and utility.

Information security handles risk management. Anything can act as a risk or a threat to the CIA triad or Parkerian hexad. Sensitive information must be kept - it cannot be changed, altered or transferred without permission. For example, a message could be modified during transmission by someone intercepting it before it reaches the intended recipient. Good cryptography tools can help mitigate this security threat. Digital signatures can improve information security by enhancing authenticity processes and prompting individuals to prove their identity before they can gain access to computer data.

II. INFORMATION SECURITY RECENT TRENDS

A. Cloud security

As the cloud environment reaches maturity, it's becoming a security target and it will start having security problems. It's possible cloud will fall victim to a tragedy of the commons wherein a shared cloud service becomes unstable and unsecure based on increased demands by companies. When it comes to cloud, security experts will need to decide who they can trust and who they

can't. Companies should develop security guidelines for private and public cloud use and utilize a cloud decision model to apply rigor to cloud risks

B. Application and data security

There is a new window of opportunity in application security, but most enterprises don't take advantage of it because of the expense. It's time to figure out the right way to evaluate the value of security and the best way to explain that to the business.
Additionally, DevOps should become DevSecOps, with a focus on security. This is a good time to marry development and operations. The time to market has shortened so much, it creates an endless connection between development and operation, which means it's important to stop running them as isolated units. This is the time to bring security to DevOps, or if the team is not internal, to ask the service provider what kind of security they provide

C. Digital ecosystems drive next generation security

Safety, reliability and privacy are also a part of cyber security. When these systems begin to have a direct physical impact, you now become responsible for the safety of people and environments. Without a handle on security, people will die. The reliability portion is essential for operation and production environments or anyone in asset-centric firms.

D. Cyber security and Internet of Things (IoT)

'Secure by design' will garner much copy but probably not deliver until 2018 or beyond. On the other hand, the next generation of AI-powered attacks will be crafty enough to emulate the behaviors of specific users to fool even skilled security personnel. This might include the ability to craft complex and bespoke phishing campaigns that will successfully fool even the most threat-conscious among us.

E. Deep learning

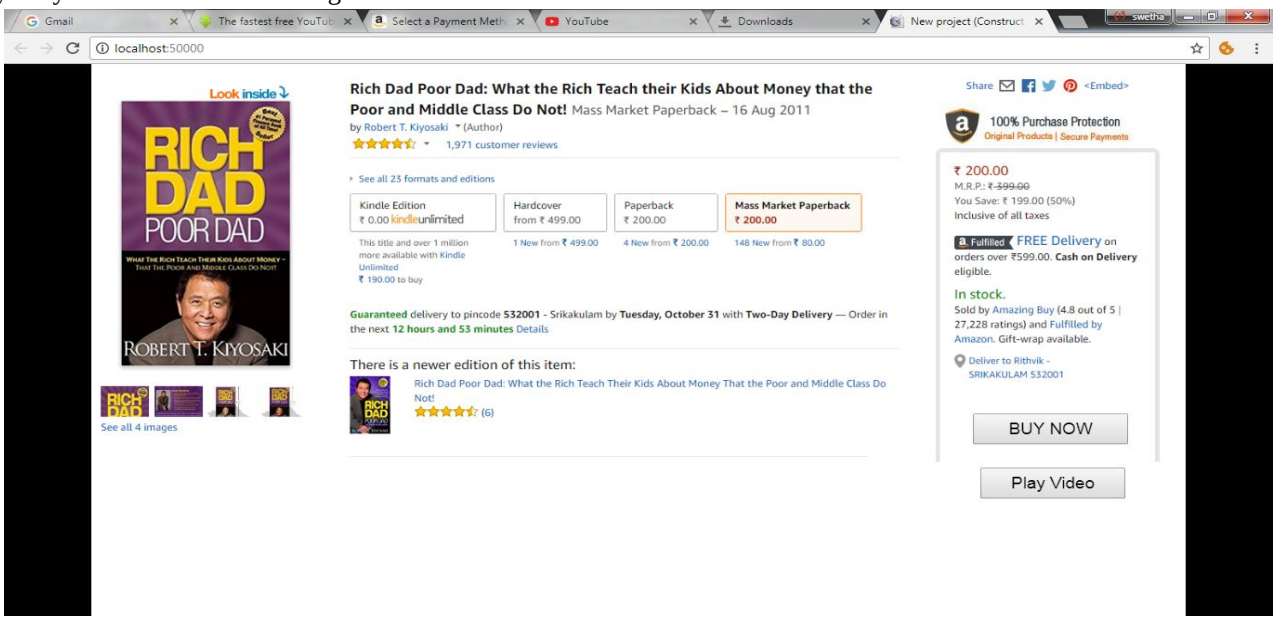
Deep learning encompasses a number of technologies, such as artificial intelligence and machine learning. "Regardless of what it's called, there a great deal of interest in it for security purposes".
Like user behavior analytics, deep learning focuses on anomalous behavior. "You want to understand where malicious behavior deviates from legitimate or acceptable behavior in The concept of artificial intelligence—the basic idea that machines could think for themselves—was made popular by British mathematician Alan Turing in the years following World War II. Turing, in many ways the father of modern computing, also created the measuring stick, dubbed the Turing Test, still used in the field of AI to determine whether a machine can be considered "intelligent." But it's been in the past 30 years or so that AI and machine learning have made great strides, graduating from the realm of science fiction and blossoming into widely used technologies with tangible real-world benefits. And at the heart of most of them is a technique called "deep learning," a catchall term that encompasses several complex and nuanced models of machine learning.
This deep learning technology manifests itself in services that many of us interface with every single day. Google, for example, applies complex algorithms and self-teaching computers to optimize listings and paid ads on its search engine results pages. Chinese search giant Baidu does the same. The goal for each is to deliver only the ads that users are most likely to click on, based on behavioral data from both individual users and groups of people with similar interests and behaviors.
And search engines aren't the only ones using AI to target our likes and preferences. Amazon and Netflix have long relied on self-improving algorithms to tailor suggested purchases, movies, and television programs to their customers.
Services like these perform a fairly simple task: they start with a basic understanding of the factors that may lead a user to perform a certain action—such as purchasing a Bluetooth headset or clicking "play" on season three of "Parks and Recreation"—and test the most efficient paths to direct a user to complete the goal. This method is known as reinforcement learning, and it's something that machines do incredibly well.

III. EXPERIMENT CONDUCTED

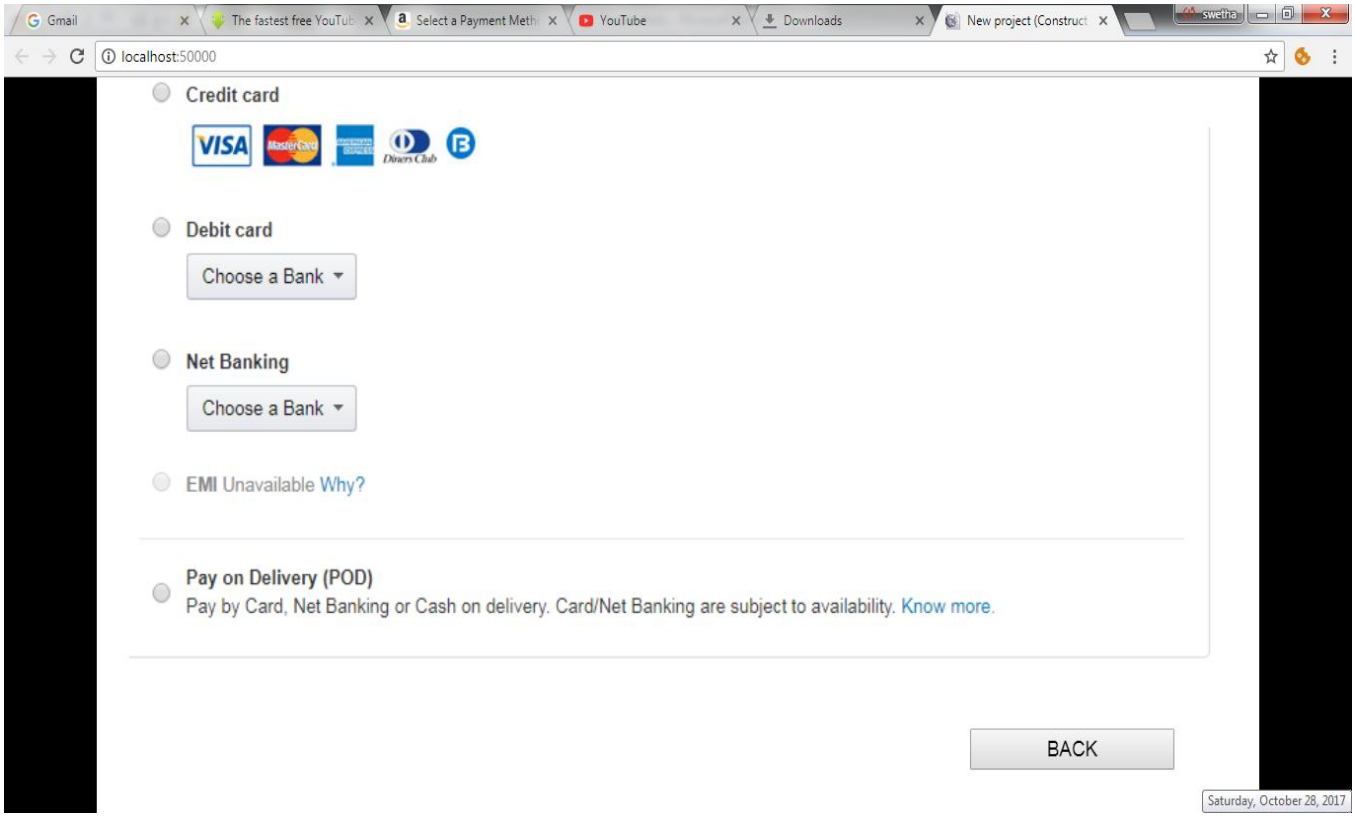
We have conducted a small experiment demo that demonstrates the information security in the above trends with the help of a
We all know about the Amazon ECOMMERCE WEBSITE there the building of website needs a lot of coding and use of all realtime examples we simply made it simple by integrating few technologies mainly the block chain technology that is prevailing now a days and the Tool we have used to authenticate data is TIBCO BW.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

The below is the screen shot that demonstrates the amazon website with a small modification the product releavant video can be displayed by an authentication message sent to the customer.



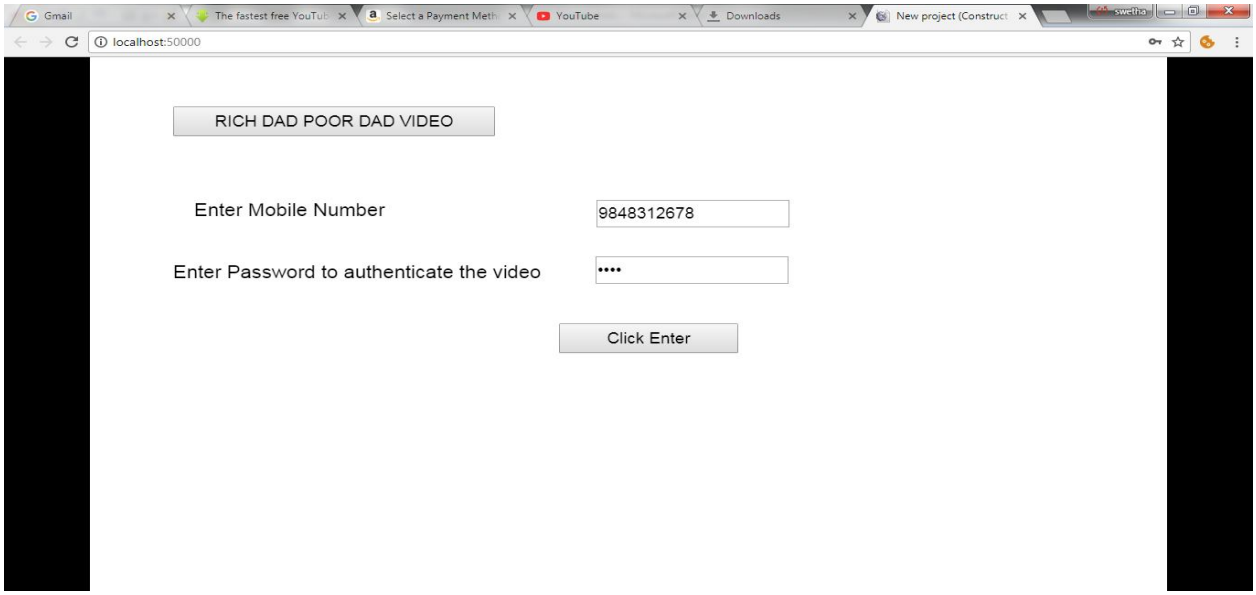
When the customer wants to buy the product the details that are enterred in the amazon web site are as usaual instead of going to the final checklist or payment we would like to integrate the BITCOIN TECHNOLOGY over here so that authentication can be done securedly and hacking can be avoided and this is under the process of evaluation and so we have kept the same authentication technology here in the below screen shot.



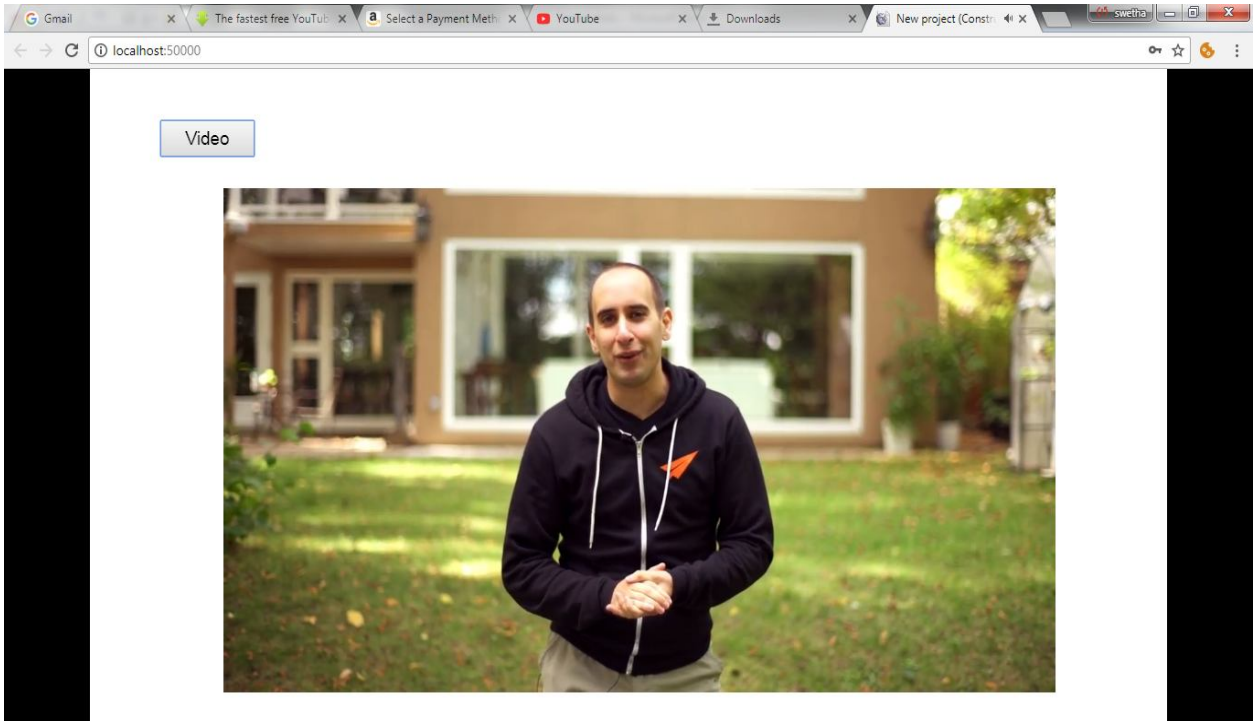
When the customer clicks the back button an authentication for the video needs to be entered by the following form and when the data entered by the customer must be validated through a network and this authentication process is a general authenticational process to access the video because now a days few products are going to copy the original products so we have used the most general way of authentication approach to a customer to watch the videos of the products

So when the customer clicks on the product the relevant video regarding the product must be entered in the following way. A network of this application has been authenticated first to gain attention of the customers. The data collected must be stored in a database and get the retrieval when and where necessary amendments are made.

A Message of the password was sent to the customer mobile through this network and the customer by getting that information can navigate to the next pages



The final step in this senario is the customer to view the video of the particular products and this can be done by clicking on the video button.We can capture few videos or we can bring many videos from the production house



IV. CONCLUSION

The above paper presented is the trial version of abstract view of security and we need to enhance this version ensembling various technologies so that technological enhancements can be made to this application and we can implement the same application that are prevailing now a days in the various sectors like banking ,movies ,bus reservations etc. We can also make a further improvement of changing the domain applications for example for security a password must be changed for every 365 days in INTERNET BANKING because there is a risk factor here. So we need to make or design an application that preserves less risk factors and that is user friendly with the help of these technologies.

V. ACKNOWLEDGMENT

We would like to thank dr.d.haritha, head of the department, c.se srk institute of technology, for supporting us in the evolution of this paper and in the research.
we would like to thank all the faculty of c.se, srk institute of technology for being with us and motivating us in each and every aspect in the enhancements of this paper.

REFERENCES

[1] Recent trends in information security-wiki.
[2] Construct 2d tutorials:
[3] TIBCO BW TUTORIAL POINT NOTES