

# CYBER SECURITY AND PRIVACY INTERNAL ATTACKS MEASUREMENTS THROUGH BLOCK CHAIN

<sup>1,2</sup>Dr.K.SAI MANOJ,<sup>3</sup>Dr. P. S. AITHAL

<sup>1</sup> Member IEEE & Postdoctoral researcher, Department of CSE, Srinivas University, Karnataka, Mangalore, India

<sup>2</sup>CEO, Amrita Sai Institute of Science and Technology and Innogeeks technologies, Vijayawada, AP, India

<sup>3</sup>Member IEEE & Vice-chancellor, Srinivas University, Karnataka, Mangalore, India

**Abstract:** Cyber Security plays critical role in privacy and now a day's its assumes an important task in the field of data security. Security concern Block chain gives best fruitful results to overcome unauthorized access and internal counter attacks operations| we propose new technique to reduce and identify internal privacy leaks and attack to measure with efficient manner. These technique very useful to cyber internal avoid attacks with accountability way and real-time environment operations. |

**Keywords:** Cloud Computing, Cyber Security, Cyber Crimes, Block Chain, Social Networks, Cloud storage, Android apps.

## 1. INTRODUCTION

Blockchain is a progressive knowledge position to transform the potential of computing and upset a few ventures with more inventive arrangements. It is open, changeless, and circulated subsequently for all intents and purposes pertinent in numerous conditions. The technology acquired huge allure from the ascent of crypto currencies yet it sees applications in numerous different areas other than money. Blockchain can be in exactly deciphered as a few cryptographically tied squares [16]. A square alludes to an information construction with three or more segments; information, the hash of the past square, and the hash of the information along with past hash. In this manner, there is a request for trust connecting blocks that be able to be utilized too guarantees the uprightness of the entire Blockchain. Ought to information in a few of the block changes, its hash resolve be changed too and this force prompt a winding impact wherever the hashes of the ensuing squares will get unacceptable. This is the reason exchanges on the Blockchain are changeless. This System is able to profoundly helpful inside contribution online protection arrangements in risky zones, for example, IOT gadgets, organizations, and information stockpiling and transmission [1-4].

Nowadayseveryone be able to send and get any sort of information that can exist an email or a audio or video presently in the break of a catch however do they yet consider how strongly client's information ID person transmit and send to forward the

following individual safely with no spillage of data. The suitable reaction lies in Cyber Security. In the present day the Internet is the quickest create system in customary on a daily basis existence. In the nearby exacting situation a variety of most recent progression is change the embodiment of mankind. Despite, outstanding to these creating advancements, we can't ensure the private data in an incredibly efficient approach and thusly, these days computerized bad behaviors are raising bit by bit [5-8]. These days more than 60% of outright business trade is through on the web [1], so this block necessary a high type of security for direct along with finest trades. In this manner, Cyber Security has become the latest issue. The degree of network safety is not immediately compelled toward checking the data inside the Information Technology business yet furthermore to a range of fields similar to the web, etc [2].

Indeed, the latest advances like appropriated figuring, distributed computing, convenient enlisting, E-business, net banking, etc in like manner need an elevated degree of protection. Because these advances grasp a few huge data concerning an individual their safety has develop into an unquestionable requirement object [11]. Updating Cyber Security and guaranteeing essential data structures are fundamental to all nations' Security along with money related prosperity and construction the Internet safer (guaranteeing internet customers) have gotten fundamental to the progress of original benefits just since administrative arrangements. The fight against cybercrime needs an expansive and safer procedure [3].

Given that specific gauges unaided can't counteract any misbehavior [4], it is significant that law prerequisite offices be permissible to examine and arraign Cybercrime feasibly [7]. Nowadays all nations and governments be forceful demanding laws on computerized insurances in order to maintain a strategic distance from the deficiency of some critical information. Every individual ought to moreover be set up on this cyber security and extra themselves [8] from these extending advanced bad behaviors.

## 2. RELATED WORK

Researchers have carried out extensive work on Block chain

and cyber security due to the great demand of security reasons in civilian applications.

### Selection of Primary Studies

A deliberate writing audit was completed in cyber security functionalities related operations under various with or without time-frame limitations. Essential examinations were recognized through a catchphrase search in important cyber attacks along with internal counter measures.

The past analysts have an alternate way to deal with take care of the security issue on every correspondences layer. Angelos M clarified that regarding network security, the main thing is the manner by which to forestall direct attacks beginning from the lower layers [10]. In view of this methodology [9], the fundamental point for Security holes to apply a lightweight security System which on different takes under genuine thought the imperfections that may happen on higher layers. This methodology for the most part makes changes to the correspondence convention. Interestingly, Saltzer et al. propose that to take care of the security issue is smarter to be more worried about start to finish security as opposed to applying lower levels of security in organizations [6].

Bosubabu Sambana et al. "Implementation of Securely Sharing Critical Information in Cloud Environment Using Mediated Certificate less Encryption System", we propose a public key encryption blueprint for the age of mystery key along with encode the information utilizing that key [11]. In the age of mystery keys, utilizing public key force inspecting conventions. Another idea is encryption and decoding of information utilizing information encryption standard computation. As a result of executing those ideas can advance the effectiveness and protection of giving shared information in cloud storage [18].

Explicitly comparable to the utilization of Blockchain to the issue of network protection [12][13], to the most awesome aspect of our insight, there gives off an impression of being extremely restricted Systematic Literature Reviews (SLRs). Quite possibly to analyze the various research papers for better way to understanding working principle and internal counter measures with inside and outside attacks for real time environment with literature review approach [7].

In our observation, this examination gives significant foundation to individual analysts who may be enthusiastic on the Blockchain base organization along with organization Security [9]. Aside from it, a small number of observations according near Block and its extrageneral outcome include additionally be circulated and resolve these issues on security beneath to analyze the smart contrasts connecting the blocks chosen through the creator and our examination [16].

Yli-Huumo et al. led a SLR in 2016 to figure out what examination outcome have been distributed corresponding toward overall idea of Blockchain Technology. They

prohibited lawful, monetary with administrative exploration on or after their audit as well as zeroed in on identification about Blockchain Technology. They discovered 80% of the examination documents center around Bit coin development, specifically on a typical subject of safety measures and protection. The applications for Blockchain have enhanced, so our exploration hopes to examine on explore working survive explicitly with respect to network protection and Blockchain applications [9].

Bosubabu Sambana et al., "Block chain approach to cyber security vulnerabilities attacks and potential Countermeasures" and he proposed a couple of safety specialist estimate to the inborn cryptographically environment of the Blockchain system be pleasant to contradict reliable hacking and security perils. Regardless, past assessments on the affirmation and assurance of Blockchain Technology have demonstrated that a couple of uses have capitulated to thriving computerized attacks. On account of the increasing revenue in support of advanced cash along with its existing security challenges, past examinations haven't focused on Blockchain Technology network protection weaknesses comprehensively [16].

Cybercrime is a name for whichever criminal conduct to utilize computers as its essential techniques for cost along with theft. The U.S. Division of Justice becomes the importance of cybercrime toward join any criminal conduct that utilizes a PC for the limit of verification. The creating overview of cybercrimes fuses infringement that has been made possible by PCs, for occurrence, coordinate interferences and the dispersal of PC contaminations, similarly as PC based assortments of accessible bad behaviors [7], for instance, discount extortion, following, annoying, and manipulation through scare tactics which contain grow to be as a critical issue to people and nations [4].

Privacy and security [32] of the information resolve reliably be top wellbeing endeavors to any association deals with. We are earlier than long confronting a day by day reality with the end goal that all the information is kept up at a high level or an advanced design. Casual correspondence districts give a break where clients have an assurance that each and every one is superior as they help out friends and family. On account of domicile clients, digital crooks would carry on centering during electronic systems administration media regions to receive outstanding information. Social Systems organization just as during bank trades an individual should take all the important safety efforts [5].

Development and restorative administrations head the country over, US Silicon valley bank identified with the purpose of associations acknowledge cyber attacks are a certified risk near together their records along with industry progression [12][14][16].

- 75% of associations are keeping up or extending their network safety property and of individuals, half are

growing wealth focused on online attacks per year

- The larger piece of associations beprepared in favor advanced attacks arise
- Simply 47% is absolutely sure about the safety of their in sequence along with yet more uncertain regarding the wellbeing endeavors of their associates.

At present, this paper passed the stage if potential cases:

- a) Take on surfing is referenced with regards to an observational assault on a confirmation technique
- b) Acknowledge-based strategy is analyzed, along with the creators be dubious concerning whether accept surfing be thought of,
- c) Take on riding attack are tended to external a few verification technique examinations

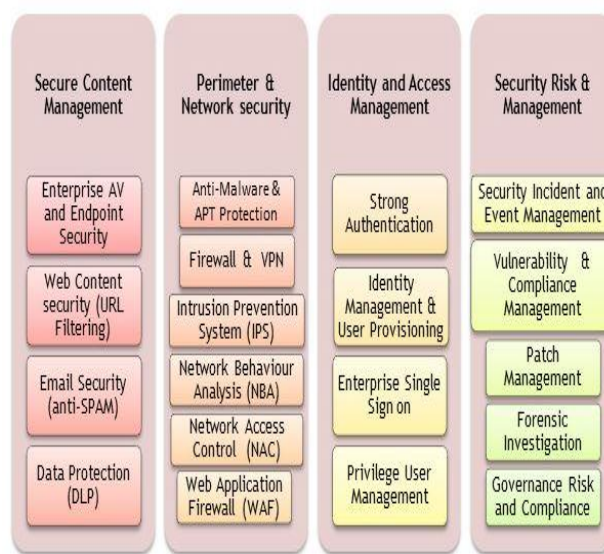


Figure.1: Cyber Secure and Network Identity Management

The below data gives full clarifications on various security mechanisms [6]

Information Security represents to when information is very still or moving, associations of all sizes need the correct assurance set up to look after security. Information security arrangements include:

- **Data misfortune anticipation:** Discover where information is put away, comprehend its area, and screen its utilization to counteract expensive information breaks.
- **Full circle encryption:** Regardless of whether information is put away physically, essentially, or in the cloud, encryption arrangements guarantee secrecy and information trustworthiness.
- **File respectability:** Validate the working System and application from which a client is altering a document. Understand the who, what, where, and when of setup changes.
- **Database assurance:** Database encryption, movement observing, and reinforcements, guarantee classification and accessibility of information [15].

**System Security:** It can convey a blend of the accompanying system security arrangements [17] custom-made to your association's special system foundation and arrange security arrangements include:

- **Intrusion anticipation Systems (IPS):** An IPS records organize traffic and investigate movement to counteract progressed malware dangers and multi-day vulnerabilities.
- **Firewall/bound together risks the board Systems (UTMs):** notwithstanding conventional firewall abilities (e.g., bundle sifting and VPNs), UTMs empower insurance of non-IP based inheritance gadgets which frequently control basic foundations.
- **Network get to control (NAC):** NAC improves organize security by restricting the accessibility of assets to gadgets that agree to predefined security conventions.
- **Advanced malware assurance (AMP):** AMPs discover, fix, and stop malware identified inside hierarchical systems.
- **Email, web and area name security:** DNS security augmentations channel email spam, screen web traffic for malignant destinations, and control the traffic end clients can get to [18].

**Edge Security (Endpoint Security):** Implementing these edge security arrangements gives a layer of security by observing your association's endpoints, edge security

arrangements include:

- **Mobile gadget security the board (MDSM):** MDSM manages and controls what, when, and where, clients can get to applications, diminishing the danger of unapproved get to and avoiding hierarchical information spillage.
- **Industrial control Systems arrangements (ICS):** Routers and firewalls that address SCADA and DCS control Systems, empowering resource ID and the board just as installed security [19].
- **Configuration and powerlessness the board:** Vulnerability scanners distinguish, arrange, and remediate vulnerabilities, for example, open ports and misconfigured programming designs.
- **Endpoint Assurance:** Disk encryption, have interruption security, and endpoint location and reaction arrangements guarantee the insurance of information very still and moving.
- **Asset the executives:** Understand the physical gadgets on your corporate system and get warnings when new gadgets are included [20].

**Application Security:** Only requiring your application's double code, it utilizes propelled apparatuses to recognize and remediate application vulnerabilities. These application security arrangements include:

- **The vulnerability the executives:** Manage the vulnerabilities related to in house created applications and online applications by means of checking devices, firewalls, and verifies code improvement [21].
- **Mobile application the executives:** User boycotting and white posting, conveyance the executives of utilizations to cell phones, and versatile application helplessness testing [8].

**Security Management:** Raw information alone isn't sufficient to settle on educated digital security choices. The security of the board arrangements transforms unstructured information into significant knowledge. The security the board arrangements include:

- **Security insight:** Real-time investigation of security alarms, an assortment of log data, and oversaw administrations.
- **Security comforts:** Managed administrations for seller explicit consoles [22]

Present resolve fresh assault on Android effective System base gadget, yet it won't be happening a huge scale. The authenticity tablets contribute to an alike functioning System as cell phones imply they determination earlier than extended alert by the equal malware as those stages [16][17].

The more than evaluation of Cyber Security incidents attacks 999 in Malaysia during January to June 2012 & 2013 evidently shows the Cyber Security danger and unlawful activity is raising still the security efforts be likewise growing.

### Trends changing cyber security

At this point referenced underneath are segments of the pattern that are hugely moving Cyber Security [8].

**Web servers:** The risk of attack on Web Applications to eliminate in sequence of data or to suitable malevolent system continues. Cybercriminals express their vindictive code throughout valid web servers they've undermined. Yet, in sequence of data attractive attacks, a significant number of which acquire the thought of media, are additionally a major risk [24]. Currently, we require an extra well-known emphasis on securing web servers and web applications. Web servers are mainly the finest stage for these cybercriminals to get in the order of data [23][25]. Accordingly individual must time and again utilize a more protected program, mostly throughout major connections all mutually not toward drop as a kill for these wrongdoings [9].

**Distributed compute and its administrations:** These days all small, average and huge organization is progressively receiving cloud administrations. Cloud can give gigantic probability though it ought to again and again be noticed to as the make unclear advance so as its security concern increase.

**Able's and Focused on Attacks:** APT (Advanced Persistent Threat) is an untrusted level of digital unlawful activity invention. In favor of fairly a extended time organization safety abilities [26][16].

**Portable Networks:** Nowadays we are able to boundary with anyone during some piece of the world. Yet, in favor of these portable systems safety is an exceptionally huge worry. We must time and again believe the safety issue of these flexible. Additional flexible systems are extraordinarily liable to these digital violations a great deal of be concerned have got to be in use if present must arise an incidence of their security issues [11].

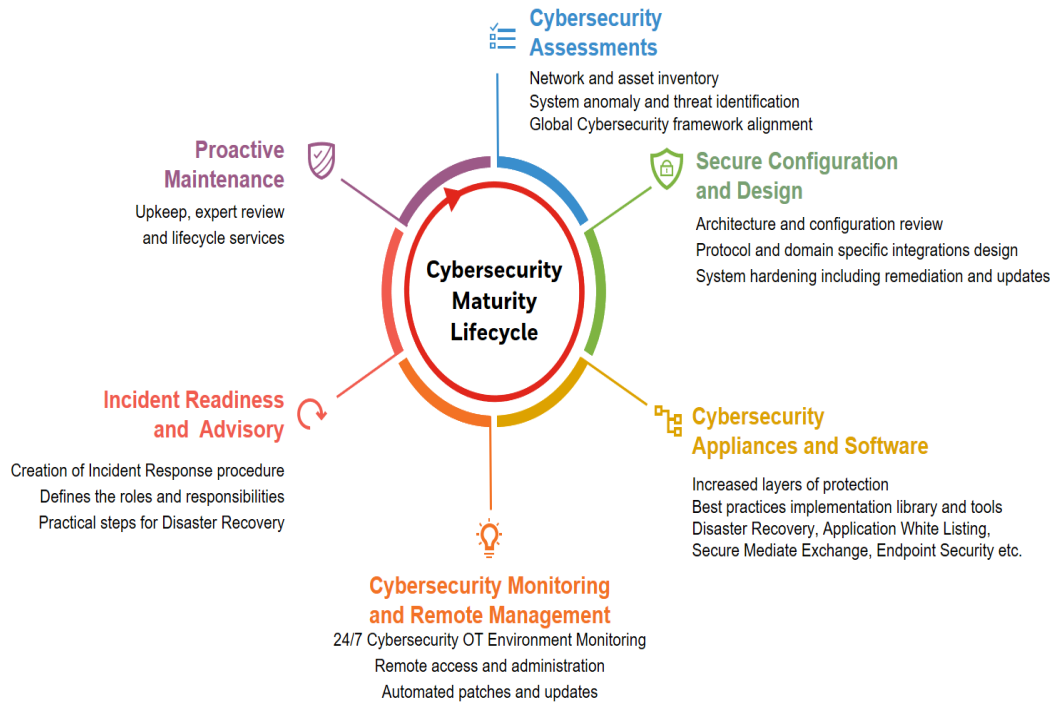


Figure.2: Cyber security Maturity Lifecycle Mechanism

**IPv6:** New web convention: IPv6 is the latest Internet gathering that is supplants IPv4, which have been the foundation of our systems what time each and every one is thought within completed and the Internet on the free. Secure IPv6 isn't basically a substance of porting IPv4 ability [27]. While IPv6 is a markdown substitute in assembly additional

IP tend toward easy to get to, there are a few extremely major changes toward the gathering which should be measured inside security strategies. It is each block enhanced near transform to IPv6 when fast as instant permit so as to diminish the danger in regards to digital unlawful activity [12].

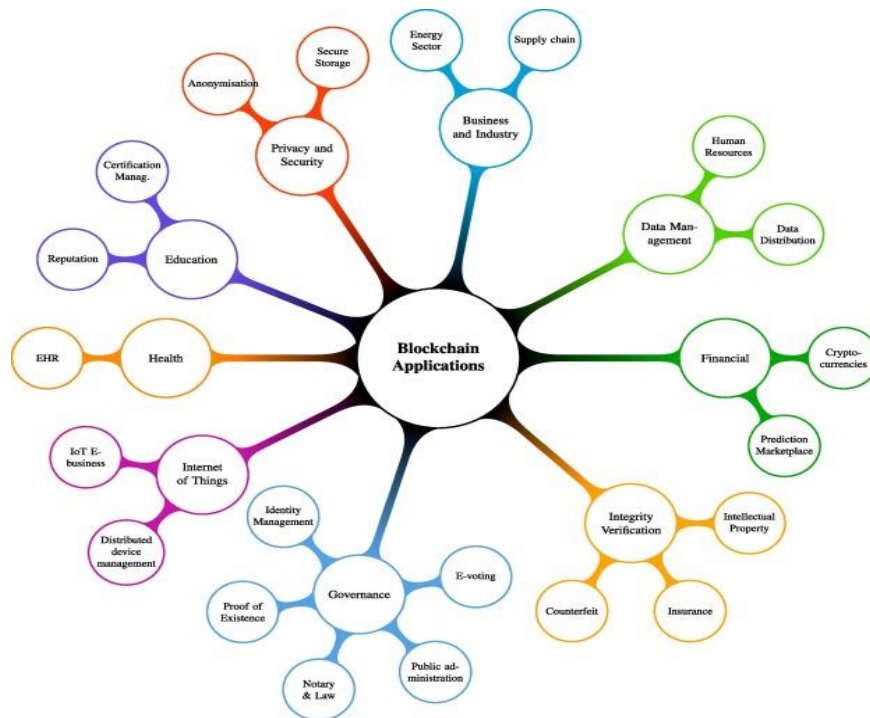


Figure.3: Classification of block chain threats and vulnerabilities.

### 3. RELATED WORK

#### Social Media in Cyber Security

As we develop into continuously Social Network and Social Media during a certainly related environment, associations should discover better way to deal with guarantee singular information [14]. Web-based life expects a colossal occupation in automated security and will contribute an incredible arrangement to entity advanced threats [16]. Online life determination between employees is taking off just like the threat of attack. While web-based life or else individual to individual communication[28] objections are approximately used by far most of them reliably it has develop into an enormous stage in favor of computerized offenders for hacking private information and taking critical information [29].

In this current reality wherever be likely to provide our own data, associations need to make sure they're likewise as fast in perceiving risks, respond logically[22][19], and keeping an essential separation from a break of several type [12]. From this time forward people should take appropriate

measures especially in overseeing on the web life to neutralize the shortage of their information [18]. The boundary of persons to give information to a gathering of persons of billions is at the center of the exacting investigation that internet organizing presents to associations. Despite empowering anyone to scatter monetarily tricky information, online person to person communication furthermore gives a comparative ability to increase false information, which is able to be just individual as unsafe [30]. The quick extend of sham data during online life is amongst the rising perils perceived inside the Global Risks 2013 report [13].

Despite the way that web-based life can be used for advanced infringement, these associations can't tolerate quitting using on the web life as it expects a huge occupation in the consideration of an association [31][16]. Regardless, relations must get this and observe the meaning of examining the data especially in Social conversation and present reasonable safety courses of action in order to continue away on or after perils. Single should manage internet organizing by using certain methodologies and the right advancements [32].

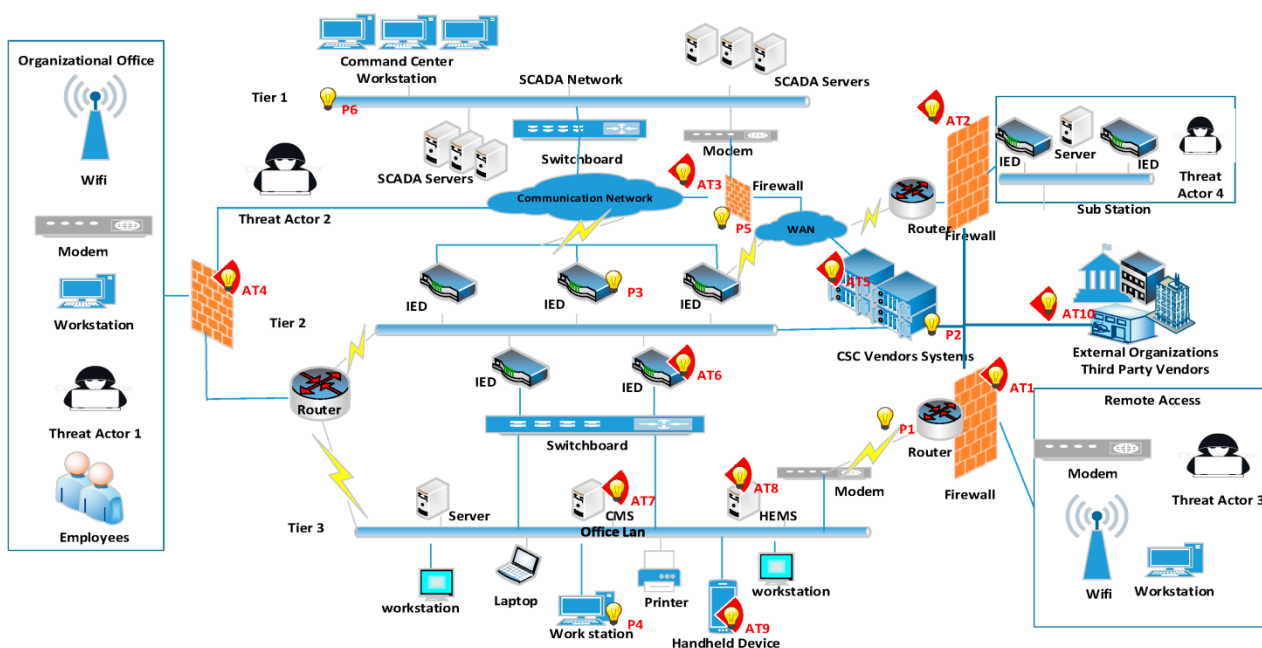


Figure.4: Block diagram of Internal Working Mechanism

### 4. RESULTS AND DISCUSSION

The appraisal of the 15 examinations demonstrated that blockchain be further practical in IOT, organization, along with information stockpiling safety [3][16][25]. The pie graph underneath sums up the discoveries whereby network, information, public key foundation (PKI), and information protection guarantee a large portion of the new Blockchain

security usage:

The second focal point of the examination is the way that Blockchain Technology is capable of utilized to improve set of connections protection [17]. Despite the fact that the current security arrangements offer honorable degrees of assurance to IT assets, they are as yet inclined to disappointment. This is on the grounds that most security

apparatuses are conveyed to work freely while getting an IT asset. As has been the situation by attack [19], Passing by the data given by the pie outline [32] over, the principal focal point of numerous analysts is the manner by which blockchain be able to advance the safety measures stood to IOT gadgets, information, as well as organizations [15].

In IOT Networks, the main security dangers are unapproved access and organize of the gadgets [31]. Block chain security arrangements be able to assist oversee access manage and information sharing for all IOT gadgets all the extra successfully. A Blockchain safety measures arrangement can be set up to guarantee dependable client distinguishing proof, verification, and information move. It might work by maintenance dispersed records about the confided in memorable associations and meetings to forestall unapproved access [16]. New associations could be set to be permitted just if countless noteworthy associations cast a ballot or check the new client. Thusly, an IoT gadget, for example, an IP camera in a residence will just allow admittance toward confide in gadgets of the family. In the event that a programmer attempts to get to the camera, the Blockchain arrangement resolve prevent contact until most of the believed gadgets vote to permit the programmer to get to the camera [33].

**Attrition of papers through processing:**

The difficulties and issues of experimental shoulder riding examine were straightforwardly researched in a recent report by Wiese and Roth. Throughout a survey of exact data bases, and the distinguish a few exploratory plan issues and talk about the ramifications they can have on the outcomes and ends drawn from the investigation. In view of that, they structure rules intended to improve future SSA tests, which they uphold by introducing a few case study analyses [18].

A small work has been done in the field to improve the estimation of this attack, explicitly. Accordingly, shoulder riding attacks are still ineffectively comprehended. Therefore, a wide range of test plans and weakness measurements have been utilized in experimental investigations, frequently without thought for the legitimacy and likeness of the outcomes. To try not to settle on specially appointed plan choices, scientists ought to be comfortable with comparable observational investigations and the ramifications their exploratory arrangements have on the outcomes [16].

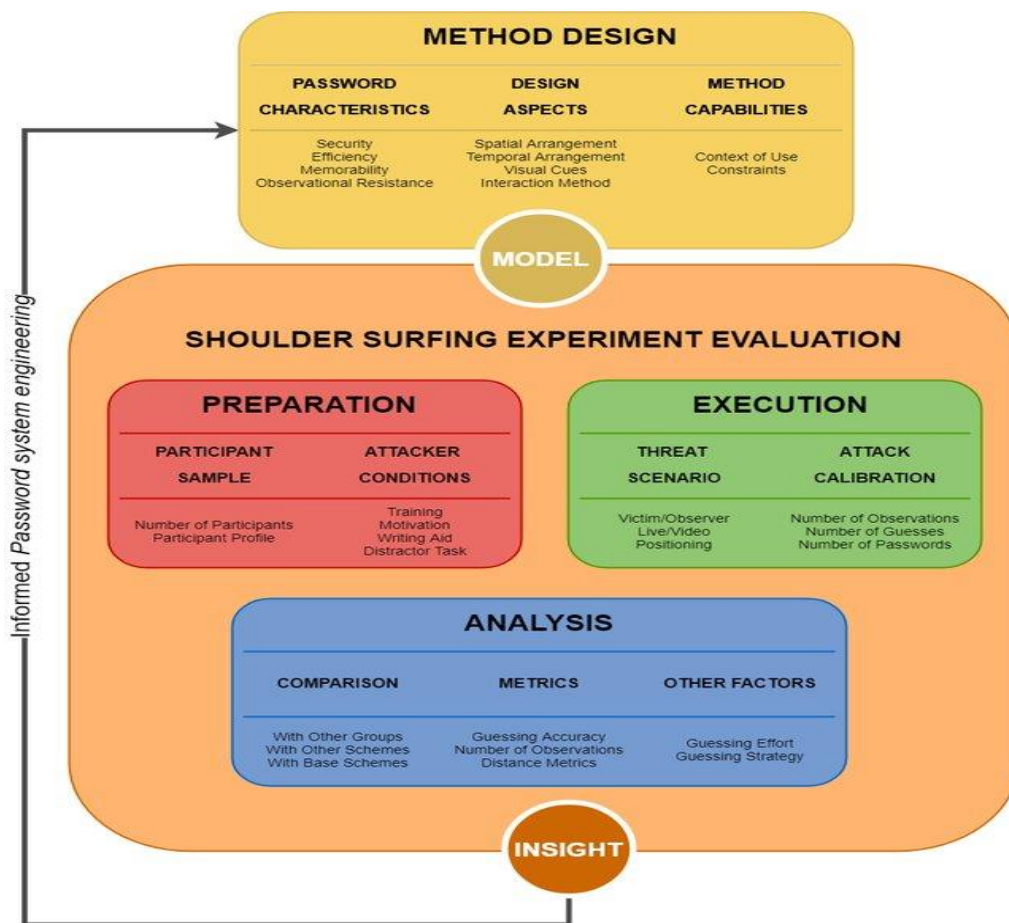


Figure.5: Attrition of papers through processing

**Data Analysis**

To get together the target of addressing the exploration question, we aggregated the information held inside the subjective along with quantitative information classes. Furthermore, we led a meta-examination of individualstobe exposed to the last information extraction measure.

In information security, the analysts recognized that the greatest shortcoming is the presence of a solitary purpose of disappointment or bargain. This prompts data or/and information theft, alteration, or misfortune. The security

scientists examined that Blockchain can be utilized to guarantee information security during its rigid groundwork [17].Becauseevery square of information shared will be hashed and associated with the following square, it will be incomprehensible for outsiders to adjust it [22]. Since just the two gatherings in the correspondence will actually want to peruse and control the information, any taken information will be unfeasible and outsiders can likewise not adjust it. Regardingnetwork communications, the security analysts distinguished to the Blockchain Technology can be utilized to present bunched Network protection henceforth forestalling unapproved associations and correspondence.

Incidents	Jan- June 2012	Jan- June 2013	% Increase/ (decrease)
Fraud	2439	2490	2
Intrusion	2203	1726	(22)
Spam	291	614	111
Malicious code	353	442	25
Cyber Harassment	173	233	35
Content related	10	42	320
Intrusion Attempts	55	24	(56)
Denial of services	12	10	(17)
Vulnerability reports	45	11	(76)
Total	5581	5592	

Table - 1: incidents in various operations on Cyber attacks

**CyberSecurityTechniques**

**Access Control and Secret Key Security:**The possibility of customer name and the mystery expression have a fundamental strategy for guaranteeing our information [18]. This may be one of the essential measures concerning to Cyber Security.

**Firewalls Validation of Information:**The records that we obtain ought to reliably be affirmed be earlier to downloading that is it must be minded the remote possibility that it has happening from a trust and trustworthy cause and that they are not adjusted. Approving these information is regularly [23] completed by the antivirus g nearby in the contraptions. In this way extraordinary antivirus writing computer programs is moreover necessary to defend the devices from contaminations [21].

**Against Infection Programming:** Antivirus writing programming is a PC program that recognizes, forestall, and make a move to put out of action or expel vindictive programming programs, diseases and worms. Most antivirus programs join an Auto-Updated incorporate toengage the series to download information sequences of original contaminations with the objective that they verify for the fresh diseases when they be found. Antivirus writing computer programs is a verifiable necessity and central requirement for every system [18].

The blow table describes Cyber Security attacks on various security levels in multiple areas with projection approach.



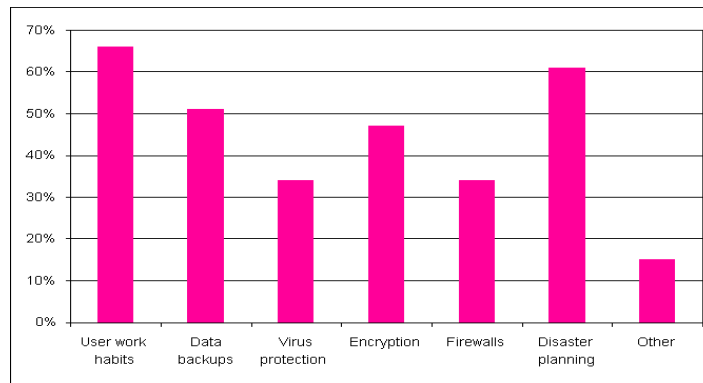


Table -2: Comparisons on Cyber security attacks on different modules

**Cyber Ethics:** Cyberethics is just the set of laws of the web. Exactly while we performed computerized ethics, presentbe incredible probability of us by the web in a fitting and safety way. The under two or three them [14]:

- Do use the Internet to give and interface with others. Email and messaging simplify it to stay in touch with friends and family, talk with work partners, and offer contemplations and information with people across over town or almost the whole way around the world.
- Internet is considered as the world's greatest library with information on any point in any part of information, so using this information in a privilege and legal way is continually essential.
- Do not work with other's records using their passwords.
- Never endeavor to send such a malware to other's systems and make them degenerate.
- When you're online never guarantee to the following individual, and never endeavor to make fake records on someone.

The above several advanced ethics one should seek after while using the web. We are continually thought authentic guidelines from our starting occasions the comparable here we apply on the web.

AI and/or Machine learning approaches are customarily partitioned into three general classifications, contingent upon the idea of the "sign" or "input" accessible to the learning System:

- **Supervised learning:**The PC is given model sources of info and their ideal yields, given by a "educator", and the objective is to get familiar with an overall principle that guides contributions to yields.
- **Unsupervised learning:** No labels No marks are given to the learning calculation, leaving it all alone to discover structure in its information. Solo

learning can be an objective in itself (finding shrouded designs in information) or a methods towards an end (highlight learning).

- **Reinforcement learning:**A PC program collaborates with a powerful climate wherein it should play out a specific objective, (for example, driving a vehicle or playing a game against an adversary). As it explores its concern space, the program is given criticism that is undifferentiated from remunerations, which it attempts to maximize. [3]

From that point onward, we will talk about some essential devices from insights and likelihood hypothesis, since they structure the language wherein many AI issues should be stated to get amiable to tackling [18]. At long last, we will layout a bunch of genuinely essential yet successful calculations to tackle a significant issue, to be specific that of characterization [29].

Taste of Machine Learning Machine learning can show up in numerous appearances. The last is vital in the event that we need to try not to waste time for each new application. All things considered, a large part of the specialty of AI is to diminish a scope of genuinely divergent issues to a bunch of genuinely tight models. A significant part of the study of AI is then to tackle those issues and give great certifications to the arrangements [19].

By using CNN to analyze and verify the malwares in entireinput units (c\*k\*k) to [23][24]modification required during the transactions process done by the connected to all output all units through fully connected Layer and categorization into 2D (2\*2) and 3D (3\*3) structured data blocks are connected to convolution layer for automated filtering bad inputs [25].

**Max-Pooling Layer:**

A pooling layer is frequentlysupplementary after a ReLU. At what time performing convolutions by a littlestep, the open fields overlap and the inform-

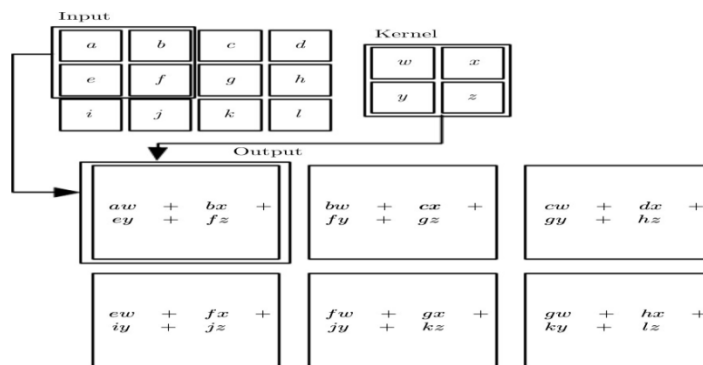


Figure .6: Block diagram of operational procedures.

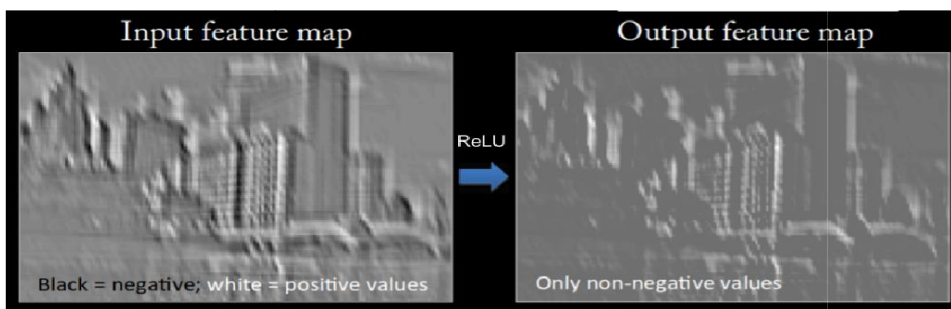


Figure .7: The result of a ReLU opening happening a characteristic Mapping.

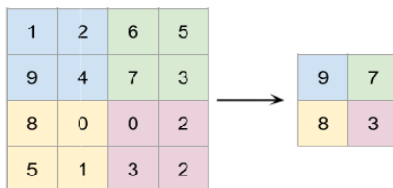


Figure.8: Example of a Max-Pooling operation with kernel and stride of size 2 × 2 matrices.

**Variable importance:** It very well may be attractive to figure out which factors and gatherings of factors contribute most to prescient ability. Significance measures were created with regard to arbitrary woodlands (Breiman2001). Applied to sacked assessors, these insights measure the decrease in exactness when a variable or set of factors in the out-of-pack test is arbitrarily permuted. Arbitrary per-change obliterates their connection with the result and with factors with which they associate, delivering them uninformative. We register these measures for each set of factors as the normal MSE contrast across five arbitrary

changes [15].

These are plotted in figure 6 of the everyday climate factors; those deliberate in mid-summer are generally significant by this measure, especially day by day precipitation, and least relative stickiness during the hottest piece of the year. The last is predictable with the discoveries of Anderson et al (2015) and Lobell et al (2013), who show that one of the fundamental components by which high temperatures influence yield is through their effect on water request [20].

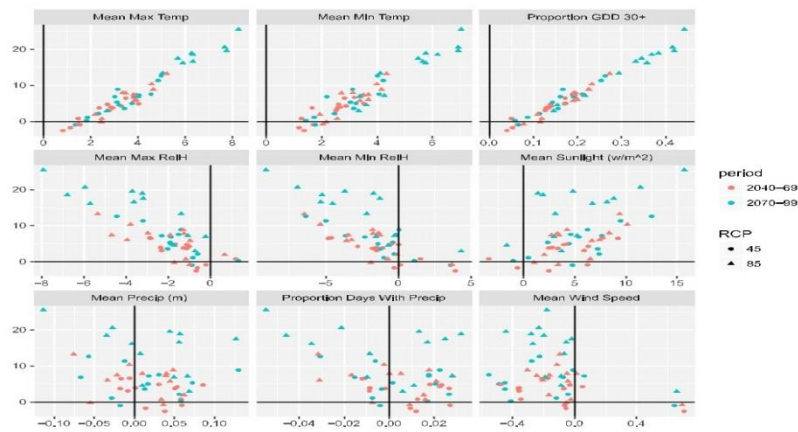


Figure.9: security Leakages in various areas in existing environment

## 4. CONCLUSION

Cyber Security is a terrific subject with the aim of resolving elsewhere unidentified and unauthorized access are occurred during data transmission and to be increasingly virus attacks done by the world is receiving deeply interconnected, with systems being utilize to do essential connection everywhere. Digital wrongdoing keep on traveling down different behavior by every year that passes consequently do the safety of the data. The most recent years and worrying advancement of these updated cyber attacks, beside the new digital devices and create dangers that happen to expose every day. In this paper we analyze the various operations with significant attacks calculations with cyber real-time environment by using lock chain approach security for internal attacks measures along with Fraud prevention and detection mechanisms are required as an add-on to BT to ensure that trustworthy and privacy-preserving attributes of the users are maintained

## REFERENCES

- [1]. A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.
- [2]. Cyber Security: Understanding Cyber Crimes-Sunit Belapure Nina Godbole
- [3]. Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.
- [4]. A Look back on Cyber Security 2012 by Luis corróns – PandaLabs.
- [5]. B sangamithra et.al, “A comparative study on a privacy protection in personalized web search”, Materials Today: Proceedings (Science Direct), <https://doi.org/10.1016/j.matpr.2020.11.148>, January 2021.
- [6]. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013, Page nos.68 – 71 ISSN 2229-5518, “Study of Cloud Computing in HealthCare Industry “ by G.Nikhita Reddy, G.J.Ugander Reddy
- [7]. IEEE Security and Privacy Magazine – IEEECS “Safety Critical Systems – Next Generation “ July/ Aug 2013.
- [8]. C Sushama et.al, “Privacy and security issues in the future: A social media”, Materials Today: Proceedings (Science Direct), <https://doi.org/10.1016/j.matpr.2020.11.105>, January 2021.
- [9]. CIO Asia, September 3<sup>rd</sup>, H1 2013: Cyber security in malasia by Avanthi Kumar.
- [10]. M Subhan et.al, “Providing Privacy Towards Personalized Web Search “in International Journal of Applied Engineering Research (IJAER) © Research India Publications July 2015 ISSN 0973-4562 Volume 10, Number 10 (2015) pp. 27393-27405.
- [11]. Ira, M., K. Aoki, E. Oshima, and H. Matsuyama. 1985. “An algorithm for diagnosis of system failures in the chemical processes”, Comp. Chem. Eng. 3, 489-493.
- [12]. D Ganesh et.al, “A Dynamic and adaptive learning mechanism to reduce cross layer attacks in cognitive networks”, Materials Today: Proceedings (Science Direct), <https://doi.org/10.1016/j.matpr.2020.11.143>, 31 December 2020.
- [13]. Mas, C. and P. Thiran. 2001. “An efficient algorithm for locating soft and hard failures in WDM networks”, IEEE Journal on Selected Areas in Communications. 18(10), 1900-1911.
- [14]. M S Kumar et.al, “ An efficient Blockchain-based IIoT System for Transparency and Concurrency Mechanism”, Journal of Critical Reviews, Vol 7 Issue 13, 2020, ISSN 2394-5125
- [15]. Rao, N. S. V. 1993a. “Computational complexity issues in operative diagnosis of graph-based systems”, IEEE Transactions on Computers. 42(4), 447-457.
- [16]. C Anitha et.al, “An Appraisal on privacy preserving mining of association rules “ at International Journal of Computer Applications, I(0975 – 8887) Volume 18– No.5, March 2011.
- [17]. M S Kumar et.al, “ Process innovation methods on business process Reengineering”, international journal of innovative Technology and Exploring Engineering, vol 8 issue 11, ISSN 2278-3075, PP: 2766-2768.
- [18]. Rao, N. S. V. 199b. “Expected-value analysis of two single fault diagnosis algorithms”, IEEE Transactions on Computers. 42(3), 272-280. Rao, N. S. V. 2002, “Nearest

- neighbor projectivefuser for function estimation”, Proc. Int. Conf Information Fusion.
- [19]. Rao, N. S. V. and N. Viswanadham. 1987. “Fault diagnosis in dynamical systems: A graph theoretic approach”, Int. J. of Syst. Sci. 18(4), 687-695.
- [20]. Shankar, M., N. S. V. Rao, and S. Batsell. 2003. “Fusing intrusion data for detection and containment, Proc. MILCOM.
- [21]. S. Staniford. 2003. “Containment of Scanning Worms in Enterprise Networks”, Technical report, Silicon Defense. Weaver N., V. Paxson, S. Staniford, and R. Cunningham. 2003. “Ataxonomy of computer worms”, WORM.
- [22]. Alex. R. Mathew , Cyber Security through Blockchain Technology , International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-1, October 2019
- [23]. Bosubabu Sambana,” Block chain approach to cyber security vulnerabilities attacks and potential Countermeasures”, International Journal of Security and Its Applications, ISSN: 2207-9629 IJSIA, Vol. 14, No. 1 (2020), pp.1-14, <http://dx.doi.org/10.33832/ijasia.2020.14.1.01>
- [24]. Bosubabu Sambana, “Internet of Things: Applications and Future Trends”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 3, March 2017, ISSN (Online): 2320-9801,
- [25]. Bosubabu Sambana, “Identifying Datasets by Pattern Recognition Techniques using Neural Networks” Asian Journal of Computer Science and Technology ISSN: 2249-0701 Vol. 6 No. 1, 2017, pp.34-39.
- [26]. Bosubabu Sambana, “Signal Processing and Display of Linear Frequency Modulated Continuous Wave Radar on a Chip” Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, Special Issue, NCETC-17, April 2017.
- [27]. Bosubabu Sambana , “An Artificial Intelligence Approach to Social Networks Agent Task Scheduling Analysis in Map Reduce for Sentiment Opinion Analysis” , 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (IEEE-iSSSC 2020)
- [28]. Bosubabu Sambana et al. “Implementation of Securely Sharing Critical Information in Cloud Environment Using Mediated Certificate less Encryption System”, International Journal & Magazine of Engineering, Technology, Management and Research, ISSN No: 2348-4845, Volume No: 2 (2015), Issue No: 11(November). <http://www.ijmetmr.com/olnovember2015/BosubabuSambana-MulaSudhakar-A-1.pdf>
- [29]. Bosubabu Sambana, “An artificial intelligence approach to fake currency detection system”, International Journal of Signal Processing, Image Processing and Pattern Recognition, ISSN: 2207-970X, IJSIP, Vol. 12, No. 3
- [40]. Arts, Sciences and Engineering (IJOAASE), 6(13), 1-9. (2019), pp.1-16 <http://dx.doi.org/10.33832/ijcip.2019.12.3.01>.
- [30]. Shoulder Surfing Experiments: A Systematic Literature Review. Available from: [https://www.researchgate.net/publication/343978396\\_Shoulder\\_Surfing\\_Experiments\\_A\\_Systematic\\_Literature\\_Review](https://www.researchgate.net/publication/343978396_Shoulder_Surfing_Experiments_A_Systematic_Literature_Review).
- [31]. Bosubabu Sambana, "Integrative Spectrum Sensing in Cognitive Radio using Wireless Network", Springer Nature Conference - International conference on Remote Sensing for Disaster Management (ICRSDM-2017) during 11-13 October 2017 at Andhra University-Visakhapatnam. First Online: 24 June 2018, Publisher Name: Springer, Cham. Print ISBN: 978-3-319-77275-2, Online ISBN: 978-3-319-77276-9
- [32]. Bosubabu Sambana, " Air Pollution Monitoring and Prediction System using the Internet of Things " , International Journal of Research and Development in Engineering Sciences , ISSN:2582-4201 , Volume: 2, Issue: 3 , Year: 2020
- [33]. Bosubabu Sambana, “ Smart Agricultural activities Monitoring and Control system using an Internet of Things” , Journal of Xidian University, ISSN No:1001-2400 , Volume-14 Issue-7, July 2020,Page No: 1645 – 1654.
- [34]. Manikandan, R and Dr.R.Latha (2017). “A literature survey of existing map matching algorithm for navigation technology. International journal of engineering sciences & research technology”, 6(9), 326-331.Retrieved September 15, 2017.
- [35]. A.M. Barani, R.Latha, R.Manikandan, "Implementation of Artificial Fish Swarm Optimization for Cardiovascular Heart Disease" International Journal of Recent Technology and Engineering (IJRTE), Vol. 08, No. 4S5, 134-136, 2019.
- [36]. Manikandan, R., Latha, R., & Ambethraj, C. (1). An Analysis of Map Matching Algorithm for Recent Intelligent Transport System. Asian Journal of Applied Sciences, 5(1). Retrieved from <https://www.ajouronline.com/index.php/AJAS/article/view/4642>
- [37]. R. Sathish, R. Manikandan, S. Silvia Priscila, B. V. Sara and R. Mahaveerakannan, "A Report on the Impact of Information Technology and Social Media on Covid-19," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 224-230, doi: 10.1109/ICISS49785.2020.9316046.
- [38]. Manikandan, R and Dr.R.Latha (2018). “Map Matching Algorithm Based on a Hidden Markov Model for Vehicle Navigation" International Journal of Advanced Technology in Engineering and Science, 6(6), 36-42.
- [39]. Manikandan, R and Dr.R.Latha (2018). “GLOBAL POSITIONING SYSTEM FOR VEHICLE NAVIGATION" International Journal of Advances in