Security Systems across Diverse Domains a Technical Review

Abhishek Mazumdar
Dept. of Electronics and Telecommunications Engineering
K.J Somaiya College of Engineering, Vidyavihar, Mumbai, India

Chetna Singh
Dept. of Electronics and Telecommunications Engineering
K.J Somaiya College of Engineering, Vidyavihar, Mumbai, India

ABSTRACT

The Internet is one humongous pool of information. With the advancement of the current digital age , more and more technologies are being developed, launched and used over the internet. But the internet is not a secure space. It is under cyber siege at all times, where attackers have their eyes on this pool of information. These vulnerabilities of the internet are transferred to all the prevalent technologies that use the internet as medium to establish a communication network. This has established a clear concern about the privacy and security risks that entail the Internet. On traversal through several modern age technologies such as Social Media, E-Commerce, Cloud, Internet of Things and Finance, an attempt is made at understanding the vulnerabilities of each of those technologies and the security mechanisms established to mitigate these security threats and concerns. Security Systems and technologies are an important aspect of the Internet that the world is shifting its focus towards this newly found objective as the threats rise day by day.

General Terms

Information Security, Cloud Security, Social Networking, E-Commerce, Internet of Things, FinTech, Blockchain, Merkle Tree

Keywords

Information Security, Cloud Security, Social Networking, E-Commerce, IoT, Finance, FinTech, Security Systems, Cybersecurity, Blockchain, Merkle Tree

1. INTRODUCTION

In the world today, there is an exponential rise in technology and use of automated systems in most of the industries prevalent. These technologies and systems store a large amount of data and information that are changing continuously in volume, monitoring and storing the minute activities taking place, we call it big data, and many businesses, industries, financial markets, world economy and to magnify it , even day to day activities rely on this data.

But with this surge in technology there is also a parallel increase in the security threats. Large amounts of data have been stolen, manipulated or even destroyed using several malwares, ransomwares and other cyber security attacks and these have not only caused several industries to lose billions of dollars but it has also been a privacy threat to confidential information. To increase the concern, these security threats are mutating rapidly. Everyday newer kinds of malwares and other security threats are being discovered. With this mutation every part of a system has become susceptible to cyber-attacks.

Hence, with the focus on technology , industries and businesses have realised the need to focus on security and mitigation of these threats and hence has caused an increase in the Importance of security systems today. Billions of dollars are being spent to acquire security technologies and services by the industries, businesses, etc and research on these security systems is at its peak. Professionals are hired to protect the most important part of any system, its DATA. Access control ,Anti-malware software, Anomaly detection, Application security, Data loss prevention (DLP) ,Email security, Endpoint security, Firewalls, Blockchain etc are some of the most commonly used security techniques and tools that have found their applications across several industries providing reliable and widespread security for most kinds of security threats . Hence, once being called an “extra service”, the Security systems have become the “Most important Asset” to any system. This paper discusses the security concerns and the security features enabled to mitigate these concerns in some of the major verticals such as social networking, e-commerce, finance, IoT and cloud.

2. SECURITY SYSTEMS OVERVIEW

2.1 Social Networking

2.1.1 Introduction

Social Media and Networking platforms, such as Facebook, Instagram, WhatsApp, etc have become one of the most popularly used technologies in this media age. With billions of users worldwide and a stupendous amount of data being shared every minute, it has become an integral part of our day to day lives. Personal data, images, texts, etc reach from one part of the globe to another within a few seconds and has revolutionized the world of instant messaging. But even though these platforms provide its users with this convenience, it is highly vulnerable to security risks.

2.1.2 Major Risks

The major risk for a platform of this form, is the Risk of Privacy. These platforms store the data of its users(personal information) in a central Repository/Database that continuously expands as new and new users join the platform and with the increasing activity of its existing users. [1] says that the main risk of privacy is due to the centralized architecture . These servers are a hub for personally identifiable information. [1] clearly highlights that the users have a false notion that the provider protects the information at all costs, where in reality it is sold to third-party organizations or could be stolen by hackers. Identity theft and selling of users’ data is one of the major privacies and security concerns for a social network. Most of the attacks aim at either stealing the identity of the user or infecting the system of the user. These could be executed using various fake accounts or executable media files such as videos, photos, etc. As identified by [2] ,some privacy risks that revolve around this sector such as insufficient authentication controls, cross site scripting, cross site request forgery ,phishing information leakage injection flaws, information integrity insufficient anti-automation .

2.1.3 Security Techniques

To counter most of the security concerns, Social Networking giants such as Facebook, Instagram, etc have provided with privacy features. These features allow the user to make their accounts "private" or allow them to restrict who can view their profile. This feature reduces the risk of cyber bullying and fraud over the Internet and blocks out several impersonators or bullies that may cause any harm to the user and keeps the user's personal data shared away from the reach of such entities. The privacy policies and content control protocols set , manages and controls the kind of media that reaches the end users filtering out most the inappropriate and to some extent even some of the malicious content and also controls the behavior of the users online. Many social media networks also provide two factor authentications which is notch higher than the usual user login. It asks for another security entry such as OTPs after the usual login which restricts the access to anybody other than the genuine user themselves. Hence, merely having the password does not give access to the account. Not only does this feature protect unauthorized access it also alerts the account holder of any sort of suspicious or unauthorized login and activity. From protecting the users' data and privacy at the users level these providers have also invested in security technologies such as firewalls and antivirus and professionals monitor the activity for unusual variations.

2.1.4 Conclusion

Even though providers have been successful in mitigating most of the security concerns it cannot be denied that social media is a public platform aiming to bring people together. Hence according to [1], users need to be careful about our activities, the information shared and the people interacted with. Prior to such platforms, Email and text messages(SMS) services were popularly used which was more secure due to just two people involved in the communication but now with the increase in chat rooms and online communities the risks have increased too and its applications have widened to gaming. Music ,etc. Hence, with all the security, social media still remains vulnerable.

2.2 E-Commerce

2.2.1 Introduction

The stable Internet came into existence in 1983 with the TCP/IP protocols and the world wide web (www) in the year 1989 ,which revolutionized the field of communication forever. It was capable of doing things mankind could not even imagine. It impacted all sectors revolutionizing industries, markets and, in a way ,"Everything". One such impact of the internet is the e-commerce industry. It changed the way we buy goods and the vendors sell their goods. It connected the vendors directly to the customers eliminating middlemen not only making it more lucrative for the vendors it also provided better prices and a wide range of products to the customers and reduced the time for delivery. It created a platform that brought the global marketplace into the homes, or to say, the palms of the customers today. Customers can buy anything, anywhere at any time. It amplified the reach of the smallest to the largest businesses to a global audience. The e-commerce giants today such as Amazon, Flipkart, etc. have created an ecosystem that changed an "in-line" shopping system to an "online" shopping system.

2.2.2 Major Risks

But this revolution too has its pitfalls. Privacy Concerns, auction fraud, non-delivery, credit/debit card fraud ,computer intrusions and spam emails are some of the common security threats that users face, as highlighted by [3]. This has caused the users to lose trust in this industry. There is now a fear among the users that their personal information is being sold to third party organizations opening gates to identity thefts and other misuse of private information. [3] suggests that the major threat to privacy is the fact that users' information is being stored without the knowledge or consent of the user. The web is highly vulnerable and the activity of the users are being monitored and potentially being sold ,even as you glance through this paper. Cookies and Web bugs are one of the most common privacy invading entities of the users, as identified by [3]. They track users' movements on the web and steal information off the host system. Bugs can store users' IP addresses, can manipulate files or install malicious files on a host to collect information or control a system if it is present in the server.

2.2.3 Security Techniques

Several technologies and protocols have been developed to tackle the loopholes in this virtual environment by securing and limiting the information access and securing the communication. As discussed by [3] , the Platform for Privacy Preferences (P3P) , a standard that attempts to control and minimize the amount of personal information stored by the website by alerting the user when and what kind of information is being stored. For an ecosystem like E-commerce it is not enough to just protect the information, monetary transactions are an important ingredient of this platform. Thus, encrypting the transactions is necessary. Public Key Infrastructure (PKI) is one of the popular methods to establish a secure passage for transactions based on cryptography. The main elements of the PKI are the Certificate Authority(CA), the Registration Authority(RA) and the public and private keys. To explain the concept in simpler words it can be compared to signing of a certificate, a digital certificate, issued by the CA. This certificate contains information about the key and is issued to the client requestor by the CA. The Certificate is like an ID card and is verified by the RA. The communication takes place only after the key is verified. To further secure the transactions , Transport Layer Security(TLS) is used to encrypt information ,such as credit / debit card details or bank details etc., and to ensure no information has been manipulated. Virtual Private Networks (VPN) emulate a private network providing remote access to a site without giving away information is another popular technology used for secure communication. Cookies and web bugs blocking technologies are also being developed to prevent security threats to the user.

2.2.4 Conclusion

These measures have been successful in reducing the risks tenfold and thus protecting the users' information and privacy. The e-commerce industry is one of the largest ecosystems and is connecting the globe together and this user oriented ecosystem holds large amounts of data and hence filling these security loopholes is prime.

2.3 Cloud Computing

2.3.1 Introduction

In this Technology Age, buzzwords such as "Cloud Computing" are quite prevalent. But what exactly is Cloud Computing? Putting it in simple terms Cloud Computing refers to the delivery of computational services such as storage, databases, processing power, networking etc. over the internet or, to say, “The Cloud” (Public, Private or Hybrid). It is one of the most rapidly growing technologies around the world with an enormous load of clients. The benefits this technology brings has revolutionized modern day business. At some point, acquiring IT services and infrastructure was a real challenge for any firm due to its high cost (Installation and Operating) and low flexibility. But now with the advent of the cloud, IT services have become more cost effective and flexible. Some of the benefits of cloud computing are cost optimization, faster delivery of on demand resources, security, reliability, availability ,global reach and many more. Cloud computing services(IaaS, PaaS, SaaS or serverless) are the most sought after technological services whose applications go beyond just storage, computing power and databases. They have their applications in creating and testing cloud native applications, streaming audio and video, analyzing data, artificial intelligence etc. A tech company as big as Netflix, relies on cloud services to deliver their streaming services. The tech giants like Microsoft(Azure), Amazon(AWS), Google(Google Cloud Platform), IBM(IBM Cloud) etc. have been delivering these cloud computing services to a pool of global customers.

2.3.2 Major Risks

But managing large amounts of data and services for clients globally has exposed this technology to a large variety of security risks. Some of the risks associated with the cloud are Lack of visibility into cloud data, Data Theft, Incomplete control on sensitive data, advanced threat attacks against cloud infrastructure, inability to prevent insider theft or misuse of data etc. Although there are a lot of benefits related to flexibility and cost optimization for service delivery the fact that a company's data and digital assets are at the hands of the service provider cannot be denied. With the development of Ransomwares like XCode Ghost and Goldeneye have now given attackers the tools to recognize the software valuation for SaaS(Software as a Service) and identify the provider increasing their focus on the vulnerabilities as identified in an article by McAfee[4]. It is also mentioned in [4] that the attack lies beyond just data. Many malicious attackers also steal computing resources for mining bitcoin or attacking other enterprises in the case of an IaaS(Infrastructure as a Service). As highlighted by [5], the security concerns arise not due to the virtual nature of the service but due to the resources being shared between enterprises. IDS and IPS systems can secure the internal virtual and physical machines from the environment if it is under one autonomous governance but for Cloud Computing, services are rented even shared making it more susceptible to attacks[5].

2.3.3 Security Techniques

Several standards and techniques have been developed to tackle these security issues associated with cloud computing. According to the article by McAfee[4], the three best practices for an organization to secure their cloud environments are DevOps processes, Automated application deployment and management tools and Unified security with centralized management across all services and providers. To secure the physical and software infrastructures [6] highlights the standards and processes for securing physical, storage and network environments. According to them, the TIA-942: Data Center Standards Overview describes the requirements for data center infrastructure and the cloud must meet these standards. For SaaS and PaaS services, Java Virtual Machine and isolation techniques have shown a lot of adoption and have reduced the risks for security concerns in a shared environment [6]. Data security is another important aspect of secure computing which is ensured by a Key infrastructure ensuring encryption of the data. The data is encrypted and identified to a user associating it to a public key . Extra Authentication by the cloud providers is a key method to identify the real user, such as sign ins. This funnels down the access to the user only and thus reduces malicious attacks and resource stealing of the users’ data and cloud infrastructure. There is a continuous audit of the cloud services to ensure the proper functioning and detect any anomalous activity that could raise security concerns. These audits also provide a sense of visibility to the user about the activities and the access in their cloud environment.

2.3.4 Conclusion

The adoption of cloud technology is growing in multitudes as more and more businesses come into the markets and this has caused a large load of client data to be stored in the environments itself. This has made it a potential spot for a cyber strike. Each day, a new form of cyber-attack is coming into the picture and the environment over which cloud services are provided(a network) makes it susceptible to these attacks. Hence, as newer and newer vulnerabilities rise there are many standards and technologies developed to counter them and protect the cloud environments.

2.4 Internet of Things

2.4.1 Introduction

After the Industrial Revolution (one of the most renowned examples of a technological revolution), back in the 1950s, the advancement in technology has been on an upward curve ever since. It has revolutionized industries , given them goals, perspectives, and the tools to function in a more efficient manner. In recent times, industries are putting in a lot of resources to make themselves more “automated”. But what is automation? Automation is the development and use of technologies for production, delivery of both goods and services with least human intervention. Automation has improved the efficiency, reliability and speed of the tasks that were previously performed by humans. This has given rise to many fields such as Robotics, Artificial Intelligence etc. One of the most prominent and important tools is the Internet of Things. The Internet of Things (IoT) has got its applications across a broad spectrum of domains such as healthcare, agriculture, energy, production, networking etc. making it a widely used industrial technology. IoT has also been able to make its way into the daily lives of people with the rise of smart homes and its applications in objects as small and simple as a sprinkler. IoT works on the principle of revolutionizing the manner in which humans interact. Due to the lower cost of the components used in developing these IoT systems, this technology has become one of the most widely used tools for automation. From fitness trackers and health monitors to smart homes and smart cities, the power of IoT is limitless.

Nearly 20 years ago, agriculture was majorly constituted by farmers working day and night to plough the fields, sowing and watering the crops through acres of land manually. But now, with the advent of technology, agriculture has become a science. Researchers, Scientists and engineers are closely studying the various aspects of agriculture to understand and develop new systems to improve and ease certain aspects of agriculture such as improving crop yield and automated sowing and sprinklers etc. Techniques such as Machine Navigation, Weeding and Harvesting Robotics, Remote

Sensing etc. have completely changed the way agriculture is done. Drones equipped with sensors and cameras are being used to image, map and survey humongous acres of land. Data from these drones can draw insights regarding crop health, irrigation, spraying, planting, soil and field, plant counting and yield prediction and much more. Remote sensors placed in the soil provide information about soil quality ,water content and the need for irrigation etc. There are sensors that also provide information about the weather based on several parameters and AI driven applications predict the weather in the future based on past patterns. These sensors' data aids the decision making by providing important insights and enables achieving maximum yield by sowing the right crops and providing the right environment . The use of IoT does not just end with the analytics in many systems, actuators are triggered that perform a specific task based on information from the sensors. For example, when the remote sensors sense the low level of water in a soil ,sprinklers are signaled.

Another major application of IoT extends to the healthcare industry. In recent years, the healthcare industry has shown a lot of innovation and technological development. In their paper,[7] has highlighted the need and the kind of innovation that is taking place in the healthcare industry such as Integration of health information systems, Drug safety monitoring and More high quality information to doctors and patients. The diagnostic systems and surgery techniques and technology are moving towards complete automation day by day. With higher accuracy and better insights through the diagnostic systems to the doctors and nurses and high precision robotic surgeries, this new age of "Automated Healthcare" is inevitable. The diseases that could not be easily diagnosed or were untreatable are now completely under control through these new technologies. IoT comes under great play in this new age of healthcare. In an article by Wipro[8], they have highlighted how IoT has redefined healthcare. Health Trackers and monitors have freed the limitation of a patient being diagnosed by a doctor only when in contact. It has given doctors the ability to monitor a patient's condition remotely. Hospitals and Health Insurance companies benefit from this technology as management of equipment and staff deployment becomes easier as it is easily traced and through data from these sensors health insurance companies can now identify insurance frauds and verify the claims, as pointed out by [8]. [8] also highlights the major advantages of IoT in healthcare such as Cost Reduction, Improved Treatment Faster Disease Diagnosis, Proactive Treatment ,Drugs and Equipment and Management Error Reduction. As elaborated by [10] , sensors that gather health information of the patients use gateway devices and the cloud to store the information and publishing this sensitive information can expose it to security threats. Hence, securing this transfer is necessary which can be achieved by the concept of Internet of Things (IoT) using wireless medical sensor network (WMSN). With the gradual rise of robotic surgeries, the demand for IoT is surging in the healthcare industry.

2.4.2 Major Risks

As we discussed the application of IoT in the above areas, it is noticeable that IoT devices and systems hold a lot of data and in many cases, confidential data. That is not it, IoT devices also control a lot of functions in several automated systems. Hence, this makes IoT a prominent attack site. Let us see why. Any IoT System can be subdivided into 4 layers namely sensing layer; network layer; middleware layer; and application layer.

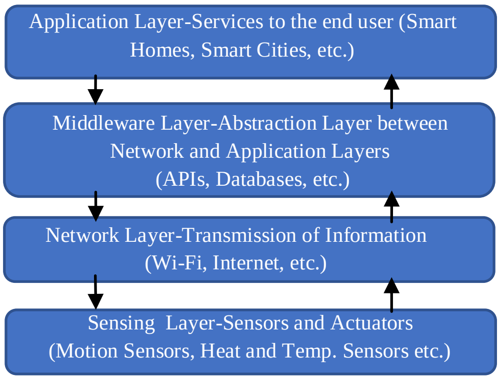
Application Layer-Services to the end user (Smart Homes, Smart Cities, etc.)
Middleware Layer-Abstraction Layer between Network and Application Layers (APIs, Databases, etc.)
Network Layer-Transmission of Information (Wi-Fi, Internet, etc.)
Sensing Layer-Sensors and Actuators (Motion Sensors, Heat and Temp. Sensors etc.)

Fig 1: IoT Layering Structure

The security threats for each of these layers are separately discussed in detail. The sensing layer consists of the sensors and actuators in IoT systems As highlighted by [11], the Sensing Layer is subjected to security threats such as sensors and actuators being replaced by a malicious node or captured by attackers giving them access to the complete IoT system, Data being leaked or altered during the data transmission phase that may lead to sensitive data being leaked to "eavesdroppers" or inaccurate results and improper services due to altered data . Other threats may include booting attacks and Denial of Service. The Application Layer corresponds to the services provided to the end user such as smart homes , smart cities etc. Security threats that correspond to this layer includes data thefts, access control intervention, monitoring of network traffic, service interruptions and remote reprogramming of IoT devices. The Network Layer corresponds to the transmission of information which includes mediums such as the internet, Wi-Fi etc. Maximum attacks take place in this layer and the threats include Denial of Service attacks, Data transit thefts, unauthorized access, Phishing site attacks and redirection of network paths or wormhole attack. The Middleware Layer corresponds to the creation of an abstraction layer between network and application layer and providing all the computing and storage capabilities such as APIs and databases etc. The security threats to this layer include SQL injection allowing the attacker to alter records in the database, Man in the middle attack that gives the attacker anonymous communication access, modification and execution of operations by the attacker and malware injection and flooding of the cloud. To concise the above threats we can clearly say that the common threats faced by IoT, circles around data thefts from the transit or database and the control of the IoT system by the attacker. This raises huge security concerns as the applications of IoT extends to homes and even cities. If an attacker gets access to the data and control of a whole city the repercussions can be disastrous.

2.4.3 Security Techniques

There have been several approaches to the security of these IoT systems such as using Machine Learning [11], Edge Computing [11], Fog Computing [11] etc. but the most prominent and popular method is Blockchain Security. In a nutshell, Blockchain is an alteration resistant and evident series of digital ledgers(blocks) that are linked(chains) to one another in a distributed fashion, without a centralized authority. Blockchain ledgers contain the Data, a hash and the hash of the previous node. Hence, any change in the block causes a change in the hash of that block that in turn makes all the other blocks ahead of the changed block invalid (provides evidence of change).

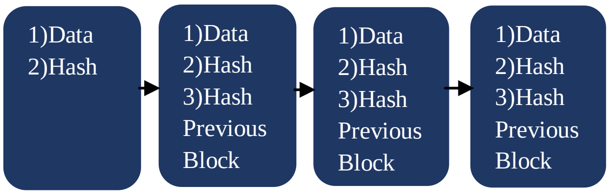

Fig 2: A Simple Structure of Blockchain

Blockchain also uses a slow process of block formation (about 10 mins) after verifying proof of work and hashes. Blockchain uses a peer to peer approach to verify the integrity of the chain. Blockchain works in a similar fashion for IoT. It contains hashes for every data transaction that takes place and is verified using a process called the Merkle Tree.

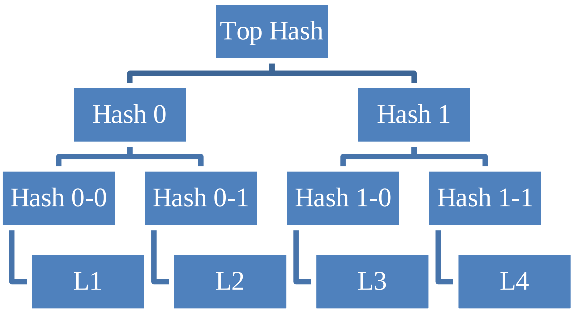

Fig 3: Merkle Tree

A Merkle Tree is a form of a binary tree that pairs hashes of consecutive blocks in pairs of 2(nodes) and in the next step pairs the next 2 resultant nodes until it gets a single hash for the complete chain which is then verified. Merkle Tree provides the advantage of verifying all the blocks' hashes by combining it to one single hash for the chain.

Other methods of verification include IOTA which requires validation of the previous 2 requests for every incoming request and cumulative weight is created for this chain of request. Higher the weight more secure is the system[11]. Blockchain can be broadly divided into 2 categories- Permissioned (Anyone can join, read and replicate from the network blocks) and Non-Permissioned(Authorized parties only and for selected set of nodes). Some of the benefits that Blockchain brings to IoT are Removal of single point of failure(Decentralization), Authorized access only, Transparency, Ensure data integrity and build trust. This makes it one of the most widely used security systems for IoT.

2.4.4 Conclusion

The Internet of Things is now being adopted by not only industries but also by nations to make their cities automated. The scope of IoT has risen from simple minute sensors and actuators to large scale industry standard Robotic maneuvers and Home and City control systems. The possibilities that IoT has to offer is beyond imagination and it has opened new horizons to the way humans interact with their surroundings. But the only flaw IoT owes its security vulnerability to is its usage over a network. It uses a network to transmit data and take actions and the control falling into the wrong hands could be detrimental and chaotic. Although this technology has the capability to change the world but it is necessary to secure it and keep it from the wrong hands.

2.5 Finance

2.5.1 Introduction

Finance is the backbone to any industry. It is not just a medium for exchanges it is also a measure of monetary value of a commodity, business, an individual , a country, or basically anything that is tangible. To reframe the earlier statement finance is not just the backbone of any industry, it is the base to pretty much any transaction. When we talk about finance we are looking at principally these following components :-

- Financial Institutions that include various forms of banks, insurance companies, credit unions and any institution related to the management and lending money.
- Financial Services that relate to Asset and Liabilities Management such as loans and savings, credit or debit card services, accountancy , stocks/bonds and investment services and other consumer finance services.
- Financial Instruments which refers to any asset that can be traded such as cash, contracts etc.
- Financial Markets refer broadly to any marketplace where the trading of securities such as the stock and bond market, forex market etc.
- And the main component Money.

But now with the propulsion of technology the face of finance has changed. The very roots of finance has been digitized and has brought finance to the palms of an individual. This digital revolution in the field has given birth to new aspects of finance such as cryptocurrency/digital currency, digital banking and payment gateways ,which we shall be discussing in detail, among many more that has changed the oriental way of operations in this sector. But this digitization has increased the risk of security vulnerabilities and due to involvement of assets and financial resources the susceptibility of a security breach in this sector is high.

2.5.2 Major Risks and Security Techniques in Online Banking

The new wave of technology has changed the complete process of delivery and procurement of banking services. The once "in line" banking service has now become completely online and has brought the pool of banking and financial services to the homes of the customers and clients providing instant service. The benefit of this new wave is not just for the customers but also to the providers who now do not have to invest in tons of space and infrastructure due to the digitization of the business. But this large scale shift of banking services over the internet has given rise to many security threats. As noted by [13], the key security threats include phishing, malware attacks, site cloning and spyware that has given rise to concerns such as services frauds, data theft, loss of money from bank accounts and many more. Online bankers know that protecting client data is a grave issue. Technologies have been developed to fill in these loopholes. Antivirus and Malware protection software, Firewalls and Secure Socket Layer(SSL) encryption blocks malicious code, unauthorized access and creates a secure connection protecting user data .Biometric Authentication is the new technology the banking industry has been investing on that uses retinal scans or fingerprints to provide authentication. This technology has seen its application in the physical banks but now this form of security is being adapted to the online services using smartphones or other appropriate gears. Multiple step authentications and cookies are actively being used to continuously recognize and authenticate the user.

2.5.3 Major Risks and Security Techniques in Payments Gateways

With the digitization of finance, more than 80% of the transactions take place online. Hence , there was a requirement of an interface in order to enable transactions over the internet which gave birth to the technology of a payment gateway. Payment gateway is a medium through which online transactions are conducted by accepting credit/debit cards and other bank details. Payment gateways are a vital part of not just finance and banking services but also the e-commerce industry today. But the usage of this technology over the internet makes it vulnerable to security threats. Many cases of data thefts, malwares and system hacks have been recorded and this has caused many entities and individuals to lose money and stolen identities have been used for impersonation or frauds. To secure the payment by the users many technologies such as Firewalls and SSL to secure the network and filter out malwares and other intrusions.

2.5.4 Major Risks and Security Techniques in Cryptocurrency

In Layman’s terms cryptocurrency can be termed as a digital asset that is used as a mode of transactions and Bitcoin is the first and most famous cryptocurrency among others Ripple, Litecoin etc. Cryptocurrency works on a peer network platform where every peer has history and information related to the transactions .When a transaction takes place it is immediately made available to the peers immediately for confirmation and once it is confirmed it cannot be changed but until then it can be manipulated or forged. But this technology too has its flaws. As highlighted by [12], the common security threats involve spoofing and phishing of payment related information, payment gateways being hacked, loss or theft of the wallet, user address spoofing etc. Another aspect of security threats in the case of cryptocurrency as brought to light by [12] is the ICO or Initial Coin Offering. Large amounts of money can be raised but there’s no guarantee of return, no risk assessment just the word of mouth as said by [12]. Cryptocurrency is protected from majorly all these risks using Blockchain. As we discussed in IoT, Blockchain works in a similar form for Cryptocurrency. All the transactions are stored in blocks as approved by the peers and each transaction is given a unique hash. These hashes are links to the next block. Hence, any change or manipulation in the transaction data causes a change in the hashes which makes the blocks forward to the changed block invalid. These hashes provide a way to verify the integrity of the data stored in the blocks.

2.5.5 Conclusion

With the digital age of financial services, various new technologies have risen which has made the process of finance simpler for the users but it has opened the vulnerabilities of the internet. Finance is a vital element of any aspect of the globe we talk about and the security threats it faces puts a lot of other functions at stake. Hence, protection of this new age finance has already shown its importance and many researchers to this day are working on protecting it.

3. CONCLUSION

With all the digitization, automation and innovation happening around the globe today the face of 95% of the industries has changed. But as we circle through each vertical in this paper, we can realize how vulnerable everything is over the internet. It can be compared to taking all your digital belongings and throwing it into one big pool called the internet which is constantly being eyed by the attackers. With more and more automation and digitization, more aspects of life tend to go over the internet. But this new wave of Digi-Automation is inevitable and a necessary step in this evolution of mankind and so the influence of the internet in our lives is only going to increase. The art of protecting this digital space has to be mastered and it has already started. The focus on security has caused several new technologies to grow in order to mitigate most of the shortcomings. Technologies such as Blockchain, Firewalls, Anti-Viruses, PKIs and Authentications, SSL, VPN, Machine Learning and other computing methods have taken this sector by storm with their immense capabilities (as tabulated in Table I) . Furthermore, many standards and protocols such as the TIA:942 and other internet protocols have been developed to ensure the safe working of the digital space. But as the security features evolve so do the attacks. Hence, authorities urge users to be vigilant and responsible about the data they share and use the new age technologies productively. In this new age of digital resources, we must use them wisely and be vigilant about the various aspects of this ocean of information, The Internet.

Table 1. Summary Table

Vertical Parameter	Social Networking	E-Commerce	Cloud Computing	Internet of Things	Finance
Major Risks	• Risk of Privacy • Insufficient authentication controls • cross site scripting • cross site request forgery • phishing • information leakage injection flaws • information integrity • insufficient anti-automation	• Privacy Concerns • auction fraud non-delivery • credit/ debit card fraud • computer intrusions • spam emails	• Lack of visibility into cloud data • Data Theft Incomplete control on sensitive data • Advanced threat attacks against cloud • Inability to prevent insider theft • Misuse of data • Theft of cloud resources	○ Sensing Layer • Sensors and Actuators replaced by a malicious node or captured • Data leakage • Booting attacks • Denial of Service ○ Application Layer • Data thefts • Access control intervention • Monitoring of network traffic • Service interruptions • Remote reprogramming of IoT devices ○ Network Layer • Denial of Service attacks • Data transit thefts • Unauthorized access • Phishing site attacks • Redirection of network paths • Wormhole attack ○ Middleware Layer • SQL injection • Man in the middle attack • Malware injection • Flooding of the cloud	○ Online Banking • Phishing • Malware attacks • Site cloning • Spyware • Services frauds • Data theft • Loss of money from bank accounts ○ Payments Gateways • Data thefts • Malwares and System hacks • Identity Thefts ○ Cryptocurrency • Spoofing • Phishing • Payment gateways being hacked • Loss or Theft of the wallet • User address spoofing
Security	• Account Privacy Options • Two Factor Authentications • Firewalls and Antivirus • Privacy Policies and Content Control Protocols • Aberrant usage monitoring	• Platform for Privacy References (P3P) • Public Key Infrastructure (PKI) • Transport Layer Security(TLS) • Virtual Private Networks (VPN)	• TIA 942: Data Center Standards Overview • Java Virtual Machine and isolation techniques • Key infrastructure • Extra Authentication (Sign Ins) • Audits and Monitoring	• Machine Learning • Edge Computing • Fog Computing • Blockchain Security	○ Online Banking • Antivirus and Malware protection software • Firewalls • Secure Socket Layer(SSL) ○ Payments Gateways • Firewalls • SSL ○ Cryptocurrency • Blockchain
Strength	Low to Medium	Medium	High	High	High
Cost	Low	Medium	Medium	High	High
Complexity	Simple	Simple	Medium	High	High

4. ACKNOWLEDGMENTS

I would like to thank my professor and mentor Prof. Chetna Singh for providing me with the opportunity of writing this technical review paper .It was due to her guidance, advice, expertise and support that I could successfully write this review paper. I would also like to thank the industry experts, researchers and other authors whose findings and articles helped me understand the respective domains and their security systems.

5. REFERENCES

[1] David Hiatt College of Arts & Sciences Regent University Virginia Beach, Virginia, U.S.A., & Young B. Choi College of Arts & Sciences Regent University Virginia Beach, Virginia, U.S.A. Role of Security in Social Networking. In (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 2, 2016 (Page 12-15)

[2] Wu He, Department of Information Technology and Decision Sciences ,Old Dominion University, Norfolk, Virginia, USA (2012),"A review of social media security risks and mitigation techniques", Journal of Systems and Information Technology, Vol. 14 Iss: 2 pp. 171 - 180

[3] Theresa A. Kraft and Ratika Kakar, School of Computer Science,University of Michigan – Flint,MI 48502, USA. "E-Commerce Security". In Proc CONISAR 2009, v2 (Washington DC): §3364 (refereed) c 2009 EDSIG , Sat, Nov 7, 11:30-11:55, Crystal 6 (Pg 1-11)

[4] McAfee. Cloud Computing Security Issues.

[5] Sasko Ristov, Marjan Gusev and Magdalena Kostoska, Faculty of Information Sciences and Computer Engineering, Ss. Cyril and Methodius University, Skopje, Macedonia. "Cloud Computing Security in Business Information Systems". In International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012 (Pg 75-93)

[6] Shubhashis Sengupta,Vikrant Kaulgud and Vibhu Saujanya Sharma,Accenture Technology Labs."Cloud Computing Security – Trends and Research Directions".

[7] Vincent K. Omachonu* Department of Industrial Engineering University of Miami Coral Gables, Florida 33124 USA ,*Corresponding Author and Norman G. Einspruch Department of Electrical and Computer Engineering University of Miami Coral Gables, Florida 33124 USA. "Innovation in Healthcare Delivery Systems: A Conceptual Framework". In The Innovation Journal: The Public Sector Innovation Journal, Volume 15(1), 2010, Article 2.

[8] Wipro. What can IoT do for healthcare?

[9] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan Department of Computer Science & Engineering American University of Sharjah, UAE. "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures ".

[10] Lobna Yehia, Ayman Khedr, Ashraf Darwish (2015) Hybrid Security Techniques for Internet of Things Healthcare Applications. *Advances in Internet of Things*, **05**,21-25. doi: 10.4236/ait.2015.53004

[11] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in *IEEE Access*, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045

[12] Mishra, Sourav & Kumari, Vasudha & Ojha, Nitish. (2018). Security issues in Blockchain and crypto currency.

[13] Jain, Anil & Sarupria, Apurva. (2019). E- Banking Problems Related to Security and, Privacy Issues along with the traits of Fraud. 10.13140/RG.2.2.22814.18244.

[14] Kuldeep Kaur , Dr. Ashutosh Pathak , Parminder Kaur , Karamjeet Kaur M.phil in Computer Application (Research Scholar), University College of Computer Application, Guru Kashi University, Talwandi Sabo, Punjab India 2Assitant Professor, University College of Computer Application, Guru Kashi University, Talwandi Sabo, Punjab, India 3Assitant Professor of Computer Sci, S.S Group of Colleges, Bhikhi (Mansa), Punjab, India 4Assitant Professor of Computer Sci, Mata Sahib Kaur Girls College, Talwandi Sabo (Bathinda), Punjab, India."E-Commerce Privacy and Security System". In Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 5, Issue 5, May 2015.

[15] Dorri, Ali & Kanhere, Salil & Jurdak, Raja & Gauravaram, Praveen. (2017). Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. 10.1109/PERCOMW.2017.7917634.

[16] Tara Salman, Maede Zolanvari, Aiman Erbad, Mohammed Samaka, Student Member, IEEE, Raj Jain, Fellow, IEEE. "Security Services Using Blockchains: A State of the Art Survey".

[17] Rajpreet Kaur Jassal1 ,Ravinder Kumar Sehgal2 1 (Assistant Professor,BBSBEC Fatehgarh Sahib,Punjab,India) 2 (Director cum Principal, Jasdev Singh Sandhu Institute of Engg. & Tech.Kauli, Patiala,India). In "Study of Online Banking Security Mechanism in India: Take ICICI Bank as an Example". In IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 1 (Jul. - Aug. 2013), PP 114-121

[18] Verma, Amit. (2013). A Multi Layer Bank Security System. 914-917. 10.1109/ICGCE.2013.6823565.

[19] J.S Vimali, Senduru Srinivasulu, Gowri. S. "IoT Based Bank Security System". In International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-2S11, September 2019.

[20] Mahmoud Ammar a,∗ , Giovanni Russello b , Bruno Crispoa a Department of Computer Science, KU Leuven University, Heverlee, 3001, Belgium b Department of Computer Science, University of Auckland, Private Bag 92019, Auckland 1142, New Zealand. "Internet of Things: A survey on the security of IoT frameworks". In Journal of Information Security and Applications 38 (2018) 8-27.

[21] Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and Privacy on Blockchain. ACM Comput. Surv. 1, 1, Article 1 (January 2019), 35 pages.