International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v11i1s.5990
***Article Received**: 08 November 2022 **Revised**: 14 December 2022 **Accepted**: 22 December 2022*

Analysing the Security Aspects of IoT using Blockchain and Cryptographic Algorithms

Rajat Verma[1, *], Namrata Dhanda[2], Vishal Nagar[3]
[1,2] Department of Computer Science and Engineering, Amity University Uttar Pradesh, Lucknow Campus, India
[3] Department of Computer Science and Engineering, Pranveer Singh Institute of Technology, Kanpur, Uttar Pradesh, India
[1, *] Rajatverma310795@gmail.com

Abstract
Technological advancement is a never-ending field that shows its evolution from time to time. In 1832, with the invention of the electromagnetic telegraph, the era of the Internet of Things (IoT) began. Within the time of 190 years, this technological domain has revolutionized IoT and made it omnipresent. However, with this evolved and omnipresent nature of IoT, many drawbacks, privacy, interoperability, and security issues have also been generated. These different concerns should be tackled with some newer technologies rather than the conventional ones as somehow, they are only the generator of those issues. Outdated Security could be an appropriate issue of IoT along with the centralized point of failure. It also possesses more concerns and challenges to tackle. On the other side, there is a visible solution to address the challenges of IoT in this developing domain of technology. The visible approach is Blockchain which acted as the backbone in securing Bitcoin in 2008, which was created by the pseudo group named Satoshi Nakamoto. Blockchain has evolved from Blockchain 1.0 to Blockchain 4.0 as the latest one depicts its amalgamation with another component of Industry 4.0 i.e., Artificial Intelligence (AI). AI will give the ability to think logically and like humans. In addition to this SMART solution, there is also an advanced cryptographical technique known as the Elliptic Curve Digital Signature Algorithm (ECDSA) which can enhance the security spectrum of IoT if applied appropriately. This paper produces a vision to enhance and optimize the security of IoT using a network peer-to-peer technology Blockchain along with advanced cryptography.

Keywords: ECC, RSA, IoT, Blockchain, Security.

I. Introduction

Cryptography is a science, involving securer and safe communication techniques that permit the original sender and the intended recipient to view the contents of the message. It is a Greek word that means hidden [1]. Cryptography was introduced years ago and involved many significant contributions and improvements from time to time. Around 600 BC when a device that was known as “Scytale”, was in use by the Ancient Spartans to send confidential messages when the battles were in progress. The device Scytale was made up of a strap of leather that was wrapped around a rod made of wood. For common people over that time, the letters that were crafted on the leather strap were meaning less and for the recipient to decrypt that meaningless data, they need to have the perfect-sized rods [2]. This marked a significant beginning in the field of cryptography. Another significant contribution of substitution cipher was used by the Roman Dictator Julius Caesar, which was a mono-alphabetic cipher in which every character in a sentence is shifted to 3 places. Here, in encryption A transforms into D, B transforms into E, C transforms into F, and so on [3-4]. The Decryption process involves the inverse of the encryption mechanism. The correct and appropriate usage of the encryption key was visualized by Giovan Battista Bellaso [5]. Cryptography comes in two variants that are Symmetric and Asymmetric Key Cryptography. The Playfair cipher, which comes under symmetric cryptography was discovered by Charles Wheatstone in 1854 [6]. Symmetric Key Cryptography is a technique that involves a single key for performing encryption as well as decryption. On the other side, Asymmetric Key Cryptography involves the use of multiple keys i.e., a Public Key and a Private Key [7]. The other name of Asymmetric Key Cryptography is Public Key Cryptography and is also related to Digital Signatures [8]. In 1918, Arthur Scherbius discovered the Enigma and made it available for commercial uses [9]. 14 years later, i.e., in 1932, Marian Rejewski visualized and understood the working of the Enigma [10]. Slowly and gradually within the next 13 years, some more developments happened and marked the end of traditional cryptography. In 1945, modern cryptography began with the mathematical theory of cryptography, an article that was at Bell Laboratories by Claude E. Shannon [11]. The early 1970s focussed on the protection of data or the facts and figures of the customers and had a group named Crypto that was created by IBM [12]. In the next 3 years, the US adopted it and made it functional as the standard and was known as the Data Encryption Standard (DES). It was in function up to 1999, until it was

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v11i1s.5990
***Article Received**: 08 November 2022 **Revised**: 14 December 2022 **Accepted**: 22 December 2022*

cracked [13]. The DES was cracked in 22 hours and 15 minutes. The DES was replaced by its successor named Advanced Encryption Standard (AES) in 2000 [14]. According to Modern Cryptography, Public Key Infrastructure (PKI) is an umbrella term for the management of public-key encryption. In Modern Cryptography RSA & ECC Algorithms used to exist predominantly originated in 1980 and 1985 respectively.

Internet of Things (IoT) is a term that can communicate and interact with many devices at the same instance with or without the intervention of human beings. The rise of IoT started in the 1800s and growing today. IoT started with the invention of the electromagnetic telegraph in 1832 [15]. The Rise of IoT is shown below in Figure 1.

Year	Journey of IoT Spectrum
1800	Long Distance Communication: The Origin
1832	Electromagnetic Telegraph
1844	Public Communication
1876	Telephones
1900s	The Beginning
1955	Wearable Computer
1973	Mobile
1990	Smart Toaster
1991	Sim Card
1999	Concept of IoT
2000	Internet Refrigerator: Blueprint
2008	Internet Protocol for Smart Objects (IPSO)
2011	Launch of IPv6
2014	Smart City
2017	Military Context
2018	HealthCare
2025	75 Billion Connected Spectrum

Figure 1. The Rise of IoT

There are enormous devices that are already present in the connected IoT Spectrum. According to research, it is expected to reach 75 billion connected devices by 2025 [16]. These devices are producing an exponential volume of unstructured data that is traversing across the globe that needs to be protected. This data is required to be protected and secured as compromising the security and integrity of data can create a huge loss to the organization. The conventional security of IoT was taken care of by Rivest Shamir Adleman (RSA), Data Encryption Standard (DES) and other encryption algorithms that are outdated and requires modern and SMART solutions. With the traditional security techniques, a large number of IoT security, privacy and interoperability issues are generated that are required to be tackled and are highlighted in the next sections. On the other hand, Blockchain is a network peer-to-peer technology blockchain whose first conceptualization was released in 2008, when it was used behind the famous cryptocurrency Bitcoin. Blockchain follows Transparency, Immutability, Decentralization and Elliptic Curve Digital Signature Algorithm (ECDSA) [17]. ECC provides the same amount of security as the RSA provides but with a much lesser amount of keys. The key generation time of ECC is less when compared to the key generation time of RSA. Blockchain follows Secure Hashing Algorithms (SHA-256) that produce the output of 64 hexadecimal characters every time until and unless a different input is provided [18]. The efficiency of keys in SHA and its different variants can also be tested using Brute force which is also highlighted in the next sub-sections. The next section illustrates the issues of IoT.

The Internet of Things: Issues

With the popularity of the IoT, issues belonging to different domains are generated as the attacks are also evolving at a speed that is lightning fast. These concerns are related to the security, privacy and interoperability aspects of the data. Protecting Data has become a most important task for enhancing the image of any organization. The Issues of IoT are highlighted in Table 1.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v11i1s.5990
***Article Received**: 08 November 2022 **Revised**: 14 December 2022 **Accepted**: 22 December 2022*

Table 1. Issues of IoT

Issues of Internet of Things	Remark
Incorrect & Unauthorized Accessing of IoT Devices	An Established System of IoT can have extreme confidence in the devices available in a LAN. Since the trust is already developed, further certification is not possible.
Frail Encryption	The Established System of IoT is vulnerable to attacks. The reason is the frail encryption.
Vulnerabilities: Bug Trusted Environment for Execution: Unavailable	The Established System of IoT acknowledges that Bugs can trigger logic bombs.
Minimal Protection of Privacy	The Established System of IoT admits that storing passwords, and sensitive information on devices leads to vulnerability.
Ignorance with Intrusion	Traditional IoT acknowledges that whenever the devices are compromised, they function normally.
Confidentiality, Authentication, and Control	Traditional IoT acknowledges that there is an absence of optimality in controlling operations in IoT devices to protect devices from cyberattacks.
Regulations	Traditional IoT acknowledges that IoT devices and software are being developed without following the laws of security, leading to misleading data
Shared Responsibility	Traditional IoT acknowledges that can with shared collaborations, IoT Security could be enhanced or not.
Fairness of Data Collection and Use	Traditional IoT acknowledges that there is an absence of rigid protocols against the collection and use of facts and figures.
Transparency & Enforcement	Traditional IoT acknowledges that there is an absence of models that enable transparency and enforcement.
Technical Risks	Traditional IoT acknowledges that there is minimal awareness of risk analysis involving risk protocols.
Configuration	Traditional IoT acknowledges that there is an absence of standard configuration concerning the scalability of IoT devices

Blockchain Technology

This Technology was discovered around 1982 by American Cryptographer David Chaum and further improved by W. Scott Stornetta and Stuart Haber in 1991 [19-20]. The first release of Blockchain was behind the renowned cryptocurrency Bitcoin. The word blockchain was a two-letter word pronounced as 'block' and 'chain' separately, but due to its popularity, it became a single word in 2016. Blockchain has evolved four times during its tenure. The initial version was called Blockchain 1.0 and was termed Bitcoin Emergence during 2008-2013. The next phase of Blockchain was called Blockchain 2.0 and was termed Ethereum Development. The Third Phase was termed Blockchain 3.0 and was responsible for the decentralized and distributed applications. The current ongoing phase is Blockchain 4.0, which is combined with Artificial Intelligence (AI) [21-22].

Blockchain has some characteristic attributes and features that can solve the issues and challenges of IoT. Blockchain has decentralization, immutability and transparency. Blockchain also involves Elliptic Curve Cryptography in addition to Digital Signatures (ECDSA). This ECC Technique is way ahead of the traditional RSA Algorithm, thus acting as an optimal solution for the security enhancement of IoT Systems using Blockchain.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v11i1s.5990
***Article Received**: 08 November 2022 **Revised**: 14 December 2022 **Accepted**: 22 December 2022*

Cryptographical Aspects:

RSA Algorithm

RSA Algorithm was developed by three colleagues, Ron Rivest, Adi Shamir, and Leonard Adleman [23]. Later on, the inventors of RSA discovered Data Security. RSA is a public key cryptographic mechanism which means asymmetric key cryptography that involves two keys, i.e., private and public keys.

Now, w.r.t. computational aspect, there is a security strength that requires a certain amount of key size. The security strength of RSA is highlighted in Table 2.

Table 2. Security Strength of RSA (Nature: Approximate) (Bits)

S.No.	Security Strength	Key Size (RSA)
1.	80	1024
2.	112	2048
3.	128	3072
4.	192	7680
5.	256	15360

When talking about the vulnerabilities, this algorithmic rule becomes weak in front of quantum computers as well as brute-force attacks [24].

ECC Algorithm

Elliptic Curve Cryptography (ECC) was invented in 1985, just 5 years later the release of RSA [25]. It provides the same amount of security while using a smaller number of keys in comparison to the traditional RSA. ECC is used predominantly in Blockchain whereas RSA protects the traditional IoT.

Now, w.r.t. computational aspect, there is a security strength that requires a certain amount of key size. The security strength of ECC is highlighted in Table 3 for better understanding.

Table 3. Security Strength of ECC (Nature: Approximate) (Bits)

S.No.	Security Strength	Key Size [ECC]	Timely Nature
1.	80	163	Approximate
2.	112	233	
3.	128	283	
4.	192	409	
5.	256	571	

Comparison of RSA & ECC Algorithm

Since RSA and ECC have dominated the cryptographic environment, the comparison between them will be a better option to find the more secure version to enhance the security of IoT. The Comparison is highlighted in Table 4.

Table 4. Comparison of RSA & ECC Keys (w.r.t. different aspects) (Nature: Approximate)

S.No.	Security concerns in bits	Size of Public Keys Represented as Bits [Minimum]		Key-Size Ratio	
		RSA (Specific)	ECC (Range)	ECC to RSA	Tenure of Validity
1.	80	1024	160 to 223	1:6	<=2010
2.	112	2048	224 to 255	1:9	<=2030
3.	128	3072	256 to 383	1:12	2030+
4.	192	7680	384 to 511	1:20	2030+
5.	256	15360	Above 512	1:30	2030+

The key-size ratio is a quintessential parameter, in defining the efficiency of a system. The Key Length & Key Generation Time Comparison of ECC & RSA is shown in Table 5 and the nature of the key computation of ECC & RSA is shown in Table 6.

Table 5. Key Length & Key Generation Time Comparison of ECC & RSA (Nature: Approximate)

S.No.	Key-Generation			
	Key-Length (Approx.) (Bits)		Time (Approx.) (Seconds)	
	ECC	RSA	ECC	RSA
1.	163	1024	0.08	0.16
2.	233	2240	0.18	7.47
3.	283	3072	0.27	9.80
4.	409	7680	0.64	133.90
5.	571	15360	1.44	679.06

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v11i1s.5990
***Article Received**: 08 November 2022 **Revised**: 14 December 2022 **Accepted**: 22 December 2022*

Table 6. Nature of Key Computation of ECC & RSA (Approximate)

Standard	ECC key	RSA key
Advanced Encryption Standard (256 bits)	512 bits	15360 bits
	Computationally Practicable	Computationally Impracticable

Therefore, one can consider, ECC (followed by Blockchain) to be a better option for security purposes than RSA in IoT or any technology.

Digital Signature Algorithm

The Digital Signature is a measure to validate the integrity of the message that involves the use of a signing algorithm and its decryption. The Algorithm initiates with the input which is fed into the hashing algorithm that is acting as one-way encryption, and a hash digest is generated. This hash digest act as an input to the signing algorithmic rule where the sender's private key (not compulsory) plays its part resulting in a digitally signed document from the sender side. This digitally signed document is sent with the help of the internet towards the receiver side where the public key (not compulsory and opposite) of the sender plays its part and thus performing the verification algorithm that verifies the hash digest obtained from the sender side and the hash value which is available on the receiver's side are equal or not. If they are equal, the signatures are valid and if not, some tampering is attempted that is required to be corrected at the earliest [26]. Blockchain follows the amalgamated version of ECC & DSA thus forming the ECDSA. This ECDSA is far better than the traditional algorithm of RSA & DES for IoT devices. The next section denotes of interpretation of the Brute Force technique in SHA Algorithms (SHA-0, SHA-1, SHA-256, and SHA-512).

Brute Force on SHA: The Complete Analysis

The brute force technique tries to attempt and crack all the possible combinations of a key. Here, the analysis of the possible combinations of SHA's is attempted. The different types of SHA's are illustrated below.

SHA-0: This initial version was introduced in 1993, but was released with few errors and faults so, it was quickly taken back. After this variant was taken back, its successor was released in 1995, named SHA-1, designed by National Security Agency (NSA). Both these SHA's give an output of 40 Hexa-decimal digits, whose interpretation is depicted in Table 7 [27].

SHA-1: The SHA-1 is identical to its predecessor (SHA-0) and was launched with major improvements.

Table 7. Interpretation of SHA-0 Hashing Technique (Identical for SHA-1)

Type	Bits/ Hexadecimal Digits	Attainable Combinations in Number of Bits	Number Length (Decimal Digits)	Factorial Value of Hexa decimal Digits
SHA-0 OR SHA-1	160/40	2^160= 1.461501637330902918203684832 71628301965593254297 6 × 10^48	49	40! = 815915283247897734345611 269596115894272000000000

Assumption:

- 1 Second = 1 Combination
- 1 Second = 1.6534e-6 Weeks (Obtained by Division by 604800)
- 1 Second = 3.80517e-7 Months (Obtained by Division by 2.628e+6)

Numerical Interpretations Obtained (Nature: Approximate):

- Approximate Weeks/Months for attempting Brute Force Technique on Total Combinations: 1461501637330902918203684832 7162830196559 32542976/604800= 2.41650402997834518e+42 Weeks or 5.56126345390802255e+41 Months.
- Approximate Weeks/Months for attempting Brute Force Technique on Factorial Value: 8159152832478977343456112695961158942720 0000000/ 604800= 1.34906627521147108e+42 Weeks or 3.10469706657207962e+41 Months.
- If the Brute Force Technique is speeding up by 1000x: 2.416504e+39 Weeks.
- If Brute Force on Factorial Value of Hexa Decimal Digits is speed-up by 1000x: 1.3490663e+39 Weeks.
- Feasibility of Brute Force on SHA: No.

SHA-256: This variant of SHA produces a digest of 64 Hexadecimal characters every time, and was launched in 2001. This SHA is used predominantly in Blockchain that worked as the backbone of Bitcoin. This SHA is securer and more complex in comparison to the previous variants of SHA. This SHA works well on 32-bit processors and saves bandwidth when compared to its successors such as the 512 variant of SHA [28-31]. The interpretation of SHA-256 is shown below in Table 8.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v11i1s.5990
***Article Received**: 08 November 2022 **Revised**: 14 December 2022 **Accepted**: 22 December 2022*

Table 8. Interpretation of SHA-256 Hashing Technique

Type	Bits/ Hexadecimal Digits	Attainable Combinations in Number of Bits	Number Length (Decimal Digits)	Factorial Value of Hexa Decimal Digits
SHA-256	256/64	2^256=1.157920892373161954235709850086879078532699846656405640394... × 10^77	78	64! = 1.268869321858841641034333893351614808028655161745451921988... × 10^89

Assumption:

- 1 Second = 1 Combination
- 1 Second = 1.6534e-6 Weeks (Obtained by Division by 604800)
- 1 Second = 3.80517e-7 Months (Obtained by Division by 2.628e+6)

Numerical Interpretations Obtained (Nature: Approximate):

- Approximate Weeks/Months for attempting Brute Force Technique on Total Combinations: 1157920892373161954235709850086879078532699846656405640394... / 604800 = 1.9145517400349903e+71 Weeks or 4.4060868471086381e+70 Months.
- Approximate Weeks/Months for attempting Brute Force Technique on Factorial Value: 1268869321858841641034333893351614808028655161745451921988... / 604800 = 2.09799821735919589e+83 Weeks or 4.8282645788380628e+82 Months.
- If the Brute Force Technique is speeding up by 1000x: 1.9145517e+68 Weeks.
- If Brute Force on Factorial Value of Hexa Decimal Digits is speed-up by 1000x: 2.0979982e+80 Weeks.
- Feasibility of Brute Force on SHA: No.

SHA-512: This variant of SHA generates an output of 128 hexadecimal values and is far ahead of previous SHA's in terms of collision resistance and it performs well with 64-bit processors. At present time, this variant of SHA is not in use but will surely be in use in the upcoming future. The interpretation of SHA-512 is shown below in Table 9.

Table 9. Interpretation of SHA-512 Hashing Technique

Type	Bits/ Hexa-Decimal Digits	Attainable Combinations in Number of Bits	Number Length (Decimal Digits)	Factorial Value of Hexa Decimal Digits
SHA-512	512/128	2^512= 1.34078079299425970995740249982058461274793685820592393377723... × 10^154	155	128! = 3.8562048236258042173567706592346364061749310959... × 10^215

Assumption:

- 1 Second = 1 Combination
- 1 Second = 1.6534e-6 Weeks (Obtained by Division by 604800)
- 1 Second = 3.80517e-7 Months (Obtained by Division by 2.628e+6)

Numerical Interpretations Obtained (Nature: Approximate):

- Approximate Weeks/Months for attempting Brute Force Technique on Total Combinations: 1340780792994259709957402499820584612747936582059239337772... / 604800 = 2.21689945931590541e+148 Weeks or 5.10190001387768512e+147 Months.
- Approximate Weeks/Months for attempting Brute Force Technique on Factorial Value: 3856204823625804217356770659234636406174931095902235902788284032763734025751655435606861685885073615340300518330589163475926...

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v11i1s.5990
***Article Received**: 08 November 2022 **Revised**: 14 December 2022 **Accepted**: 22 December 2022*

172932262498857766114955245039357760034644709279247692495585280000000000000000000000000000000/ 604800= 6.37600003906382964e+209 Weeks or 1.46735182559077121e+209 Months.

- If the Brute Force Technique is speeding up by 1000x: 2.216899e+145 Weeks.
- If Brute Force on Factorial Value of Hexa Decimal Digits is speed-up by 1000x: 6.376e+206 Weeks.
- Feasibility of Brute Force on SHA: No.

The Summarised Analysis of Brute Force on SHA is represented in Table 10.

Table 10. Analysis of Brute Force on SHA

S.N.	Brute Force on SHA	Result obtained w.r.t. Brute-Force
1	SHA-0 & SHA-1	Not Feasible
2	SHA-256	Not Feasible
3	SHA-512	Not Feasible

Blockchain Solutions for IoT

Blockchain technology provides modern and SMART solutions for the diverse issues of IoT. Table 11 shows the convenient blockchain solutions for IoT.

Table 11. Blockchain Solutions to IoT Concerns

Issues of Internet of Things	Remark	Property of Blockchain	Solution Achievable
Incorrect & Unauthorized Accessing of IoT Devices	An Established System of IoT can have extreme confidence in the devices available in a LAN. Since the trust is already developed, further certification is not possible.	Immutable & Protected by SHA-256	Yes, Complete.
Frail Encryption	The Established System of IoT is vulnerable to attacks. The reason is the frail encryption.	Blockchain Follows the Secure Hashing Algorithm predominantly 256 and the amalgamated approach of Elliptic Curve and Digital Signature (ECDSA).	Yes, Complete.
Vulnerabilities: Bug Trusted Environment for Execution: Unavailable	The Established System of IoT acknowledges that Bugs can trigger logic bombs.	The Environment in Blockchain is different and follows various Consensus Mechanisms.	Yes, Complete.
Minimal Protection of Privacy	The Established System of IoT admits that storing passwords, and sensitive information on devices leads to vulnerability.	Privacy is enhanced by Blockchain.	Yes, Complete.
Intrusion Inactivity	Traditional IoT acknowledges that whenever the devices are compromised, they function normally.	As Intrusion in Blockchain is encountered, The hash Values are altered highlighting that tampering is done.	Yes, Complete.
Confidentiality, Authentication, and Control	Traditional IoT acknowledges that there is an absence of optimality in controlling operations in IoT devices to protect devices from cyberattacks.	Blockchain takes care of proper authentication and control, using SHA, ECDSA etc. Blockchain offers diverse configurations that are sufficient in completing the requirements.	Yes, Complete.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v11i1s.5990
***Article Received**: 08 November 2022 **Revised**: 14 December 2022 **Accepted**: 22 December 2022*

Regulations	Traditional IoT acknowledges that IoT devices and software are being developed without following the laws of security leading to misleading data	The blockchain environment ensures security so the chances of misleading data are minimized.	Yes, Complete.
Shared Responsibility	Traditional IoT acknowledges that can with shared collaborations, IoT Security could be enhanced or not.	The blockchain consensus mechanism ensures that security is achieved in shared collaborations also. Decentralization, Immutability, and Transparency also ensure the same.	Yes, Complete.
Fairness of Data Collection and Use	Traditional IoT acknowledges that there is an absence of rigid protocols against the collection and use of facts and figures.	Blockchain ensures fairness of data collection and use and enhances privacy and security aspects.	Yes, Complete.
Transparency & Enforcement	Traditional IoT acknowledges that there is an absence of models that enable transparency and enforcement.	Blockchain ensures Transparency & Enforcement and enhances security aspects.	Yes, Complete.
Technical Risks	Traditional IoT acknowledges that there is minimal awareness of risk analysis involving risk protocols.	Blockchain minimizes technical risks, data inconsistency, and data breaches because it follows immutability.	Yes, Complete.
Configuration	Traditional IoT acknowledges that there is an absence of standard configuration concerning the scalability of IoT devices	Blockchain follows standard configuration and lightweight blockchain (future scope) can provide scalability.	Yes, Complete.

II. Results and Discussion

The textual matter represented in this paper highlights the importance of Blockchain for tackling the issues of IoT. IoT has evolved from the 1800s to the 2020s whose journey is highlighted in Figure 1. This popularity of IoT has led to various challenges and concerns for IoT devices to survive. The Issues are highlighted in Table 1 for easy understanding. The Cryptographical aspects of IoT have now become weak and require modern and SMART solutions. The Traditional IoT follows the RSA algorithm whereas the next big thing i.e., Blockchain follows ECC. The security strength of the RSA Algorithm is highlighted in Table 2 whereas the security strength of the ECC Algorithm is highlighted in Table 3. When RSA & ECC are compared various facts and figures have aroused which are illustrated in Tables 4, 5 and 6. The Complete analysis of the Brute Force Technique over the diverse Secure Hashing Algorithms is shown in Tables 7,8 and 9. Enormous values are obtained while performing the brute force technique over the diverse SHAs. The results are simple, not feasible and the brute force technique is not able to tamper with the security of systems secured by SHA Algorithms such as Blockchain. Blockchain follows the SHA-256 that generates the result of 64-Hexadecimal characters every time. The Analysis of Brute Force on SHA is illustrated in Table 10. The Blockchain solutions for IoT concerns are highlighted in Table 11 for easy grasp. Overall, the traditional methods are outdated and the Blockchain is suitable to handle the modern security, privacy and interoperability issues of IoT.

III. Conclusion and Future Scope

Industry 4.0 has seen the evolution of IoT and also the revolution caused by Blockchain. The enormous data caused by the IoT spectrum can be properly secured by Blockchain. The Evolution of IoT with its issues is highlighted in this

paper. The Introduction of Blockchain with its sub-techniques such as ECC and Digital Signatures is also illustrated in this paper. The RSA Algorithm is compared with the ECC Algorithm which is well depicted in this paper where the ECC comes out to be a winner. The Complete Interpretation of SHA with the help of the Brute Force Technique is also highlighted in this paper. The Blockchain Solutions for IoT issues are presented in a tabular form in this paper.

Additionally, the author will continue to research in the field of IoT and Blockchain which is considered a future scope.

REFERENCES

[1] Saleh, M. E., Aly, A. A., & Omara, F. A. (2016). Data security using cryptography and steganography techniques. International Journal of Advanced Computer Science and Applications, 7(6), 390-397.

[2] Roberts, W. (1843). History of Letter-writing: From the Earliest Period to the Fifth Century... W. Pickering.

[3] Kotola, B. S. (2020). Application of modulus theory to crytographic system. International Journal of Advanced Research in Engineering and Applied Sciences, 9(1), 19-33.

[4] Adhikari, M. R., & Adhikari, A. (2014). Introduction to Mathematical Cryptography. In Basic Modern Algebra with Applications (pp. 517-584). Springer, New Delhi.

[5] Tulpan, D., Regoui, C., Durand, G., Belliveau, L., & Léger, S. (2013). HyDEn: a hybrid steganocryptographic approach for data encryption using randomized error-correcting DNA codes. BioMed research international, 2013.

[6] Kaur, A., Verma, H. K., & Singh, R. K. (2012). 3D (4 X 4 X 4)-Playfair Cipher. International Journal of Computer Applications, 51(2).

[7] Lozupone, V. (2018). Analyze encryption and public key infrastructure (PKI). International Journal of Information Management, 38(1), 42-44.

[8] Verma, R., Dhanda, N., & Nagar, V. (2022). Enhancing Security with In-Depth Analysis of Brute-Force Attack on Secure Hashing Algorithms. In Proceedings of Trends in Electronics and Health Informatics (pp. 513-522). Springer, Singapore.

[9] Al-Duri, A. S. (2021). Enigma Evolution & Cryptanalysis. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(14), 5566-5569.

[10] Cawthorne, N. (2014). Alan Turing: The Enigma Man. Arcturus Publishing.

[11] Rousseau, R. (2002). Claude Shannon: scientist-engineer. Journal of Henan Normal University, 30(4), 1-13.

[12] Arnold, M., Bellamy, R. K., Hind, M., Houde, S., Mehta, S., Mojsilović, A., ... & Varshney, K. R. (2019). FactSheets: Increasing trust in AI services through supplier's declarations of conformity. IBM Journal of Research and Development, 63(4/5), 6-1.

[13] Coppersmith, D. (1994). The Data Encryption Standard (DES) and its strength against attacks. IBM journal of research and development, 38(3), 243-250.

[14] Ingle, S. S., Bhalekar, P. M., & Pathak, K. S. (2014). Using Advanced Encryption Standard (AES) Algorithm Upgrade the Security Level of ATM Banking Systems. Int. J. Res. Sci. Technol., 1(2), 1-7.

[15] Bektas, Y. (2001). Displaying the American genius: the electromagnetic telegraph in the wider world. The British Journal for the History of Science, 34(2), 199-232.

[16] Verma, R., Dhanda, N., & Nagar, V. (2022). Security Concerns in IoT Systems and Its Blockchain Solutions. In Cyber Intelligence and Information Retrieval (pp. 485-495). Springer, Singapore.

[17] Verma, R., Dhanda, N., Nagar, V. (2023). Towards a Secured IoT Communication: A Blockchain Implementation Through APIs. In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues, J.J.P.C., Ganzha, M. (eds) Proceedings of Third International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems, vol 421. Springer, Singapore. https://doi.org/10.1007/978-981-19-1142-2_53

[18] Verma, R., Dhanda, N., Nagar, V. (2023). Application of Truffle Suite in a Blockchain Environment. In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues, J.J.P.C., Ganzha, M. (eds) Proceedings of Third International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems, vol 421. Springer, Singapore. https://doi.org/10.1007/978-981-19-1142-2_54

[19] Ghosh, A., Anwar, F., Sarkar, A., Sarkar, S., Bose, S., Aditya, S., & Saha, D. (2021). Applications of Blockchain Technology in Financial & Personal Data Security. American Journal of Electronics & Communication, 2(2), 5-11.

[20] Обушний, С. М., Кравченко, Р. С., Хацкевич, Л. В., Некрасов, С. І., & Франціян, А. І. (2020). Analysis and solution of the conceptual and terminological problem of the Blockchain concept definition. European scientific journal of Economic and Financial innovation, (2), 14-36.

[21] Perera, S., Nanayakkara, S., Rodrigo, M. N. N., Senaratne, S., & Weinand, R. (2020). Blockchain technology: Is it hype or real in the construction industry?. Journal of Industrial Information Integration, 17, 100125.

[22] Shrimali, B., & Patel, H. B. (2021). Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. Journal of King Saud University-Computer and Information Sciences.

[23] Panda, M. (2014). Security in wireless sensor networks using cryptographic techniques. American Journal of Engineering Research (AJER), 3(01), 50-56.

[24] Hasanova, H., Baek, U. J., Shin, M. G., Cho, K., & Kim, M. S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. International Journal of Network Management, 29(2), e2060.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v11i1s.5990
***Article Received**: 08 November 2022 **Revised**: 14 December 2022 **Accepted**: 22 December 2022*

[25] Jamgekar, R. S., & Joshi, G. S. (2013). File encryption and decryption using secure RSA. International Journal of Emerging Science and Engineering (IJESE), 1(4), 11-14.

[26] Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). International journal of information security, 1(1), 36-63.

[27] Madhuravani, B., & Murthy, D. S. R. (2013). Cryptographic hash functions: SHA family. Int J Innov Technol Explor Eng, 2, 326-9.

[28] Kong, J. H., Ang, L. M., & Seng, K. P. (2015). A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments. Journal of Network and Computer Applications, 49, 15-50.

[29] Akinyede, R. O., Adegbenro, S. O., & Omilodi, B. M. (2020). A security model for preventing e-Commerce related crimes. Applied Computer Science, 16(3), 30-41. doi:10.23743/acs-2020-19.

[30] Rajat Verma, Namrata Dhanda, Vishal Nagar, "Enhancing & Optimizing Security of IoT Systems using Different Components of Industry 4.0." International Journal of Engineering Trends and Technology, vol. 70, no. 7, pp. 147-157, 2022. Crossref, https://doi.org/10.14445/22315381/IJETT-V70I7P216

[31] Verma, R., Dhanda, N., & Nagar, V. (2020). Addressing the issues & challenges of internet of things using blockchain technology. International Journal of Advanced Science and Technology, 29, 10074–10082.