International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-3, January 2020

Architectural Framework for Intelligent and Secure Aadhar Data Management Synchronized with both Offline and Online Transaction Systems

Chhaya S Dule, Nandini N, Rajasekharaiah K M

Abstract*: The information of the citizens identity are reposited in the national database system that demands higher degree of security features in order to combat the privacy problems associated with it. The information retained within an identity of a citizen is highly valuable as well as sensitive as it is constructed by integrating various forms of biometric trails e.g. iris, fingerprint etc along with their personal details. Aadhar is one of such initiatives by Government of India by their "Unique Identification Authority of India (UIDAI) project" that generates 12-digit random number as unique identity. The Government of India is in progressive approach to integrate various social and security related applications to Aadhar in order to achieve identification-based service provisioning. In the recent news, Aadhar details have been reported to be encountered a serious security breach that endangered the private details of the Aadhar card holders. Therefore, a robust and efficient secure eco-system is required to keep national ID database secure. This chapter aims to describe novel framework for Aadhar data privacy and storage management by adopting efficient data blockage and transformation over cloud storage using statistical method based on data embedding by blocking and transformation.

***Keywords* : Security, Internet of things, Data Security, Data Privacy, Privacy Preservation, Attacks, Aadhar Card Security.**

I. INTRODUCTION

In present times, there is a much hype of constructing smart cities that is based on upcoming concept of Internet-of-Things (IoT). Basically, IoT is all about forming a capability of network connectivity among wide number of physical devices [1][2]. It is also believed that IoT is not only about connecting physical devices like sensors but also various other form of physical devices that has certain degree of computational capability [3][4].

Revised Manuscript Received on January 30, 2020.
***** Correspondence Author
Chhaya S Dule*, Research Scholar, Department of CSE, Dr. AIT, Visvesvaraya Technological University (VTU), Belgaum, and Karnataka, India, Associate Prof, Department of CSE, K G Reddy College of Engineering & Technology, Hyderbad, Telangana-State, India Email: chhaya0671@gmail.com
Dr. Nandini N,Associate Professor, Dept of CSE, Dr. Ambedkar Institute of Technology, India,
Dr. Rajasekharaiah K M, Dean & Professor, Faculty of Information Technology, Amity Institute of Higher Eduction, Mauritius

Hence, offering comprehensive security system on such IoT devices is really a challenging task. The most significant problem of IoT related to security is mainly data encryption [5]. Applying existing encryption standards are yet to be benchmarked in association with offering IoT security. They most widely used data encryption protocols have different set of problems in relation with cyber-physical environment in IoT. Another significant security problem in IoT is related to data authentication. Owing to larger number of sensory application usage, it is quite impossible to assess the legitimacy of the rogue IoT devices in the larger network [6]. Although, there are various studies being carried out for offering different kinds of solution towards strengthening the authentication capability in IoT (e.g.[7]-[10]), but there are many reported pitfalls of the underlying concepts being used for the implementation. The next security problem associated with IoT is related to adversary model. The adversaries in cloud as well as in IoT may quite differ owing to its propagating environment. The adversaries in cloud mainly propagate using internet-based programs, while the adversaries in IoT are propagated from physical devices i.e. hardware [11]. For an example, the denial of service attack is very common in cloud-based applications while side channel attacks are common in IoT application. However, some common attacks in both are denial of service, key-based attacks, and memory-based attack. Although, there are good set of availability of research work towards resisting such forms of attacks in cloud but there is still scarcity of any robust and full-proof solution toward securing IoT-based attack. Hence, cloud-based security solutions cannot directly offer security services to IoT without undergoing significant changes in their protocol operation mode. One significant study carried out by Chauhan et al. [12] showed that authentications by any means are most essential steps of securing the communication among the IoT devices in the smart cities. The online authentication system demands certain soft-copy of user identification while offline authentication system may demand use of biometric [13]. Considering the case study of India, it can be considered that if smart cities becomes functional than certain form of user's identity-based information will be used for accessing the services. At present, Aadhar card is considered as a sole identity of an Indian citizen apart from their nationality passport [14].

However, there has been a recent new about malicious and unethical intrusion to massive Aadhar card user that has introduced a potential threat to the identity of large number of users.

It is because Aadhar card is linked with individual's bank that can offer a potential threat to their banking account in many ways. The biggest problem with the existing mechanism of repositing the Aadhar card is that all the soft copy of it is reposited in one physical system with normal security that can be cracked by anyone attacker without much effort.

There are many good possibilities to offer a solution towards this technique. The first possible solution could be to apply some forms of distributed storage with hashing that could offer better privacy standards. The recent implementation of privacy preservation protocols works best on the data over the network using distributed protocols [15]. However, such technique doesn't cater up resiliency requirement for different forms of adversaries from cyber-physical systems in IoT. The second possible solution will be to apply some typical cryptographic algorithm e.g. Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest-Shamir Algorithm (RSA),Elliptical Curve Cryptography (ECC) etc. All these algorithms are quite good enough and have been already proven to offer significant security over cloud-based application; however, they also have reported flaws [16]. The third possible solution is to evolve up with a novel encryption technique. The biggest challenge in doing so is to consider different forms of adversaries, which is not feasible and has never been done so far. The fourth possible solution will be to apply image-based encryption techniques to all the file system that are stored in the form of image. However, existing image-based security policies e.g. encryption, visual encryption, steganography etc are never tried over IoT based environment. Moreover, there are only few research-based work that has investigated considering Aadhar card; however, they are least implementation of any robust scheme that ensure data security of the Aadhar card stored in storage units in IoT system and accessed by IoT devices. Therefore, the contribution of the proposed system is to offer a simple but yet a robust solution towards data security problems of Aadhar card in IoT system. The organization of the proposed paper is as follows: Section II discusses about existing research work on data security in IoT, Section III discusses about the research problem identified from existing security techniques followed by discussion of research-based methodologies in Section IV. The algorithm discussion is carried out on Section V while analysis of result is illustrated in Section VI. The applicability of proposed study is discussed in Section VII while the study contribution is briefed in Section VIII.

II. REVIEW OF LITERATURE

This section discusses about various research work carried out towards data privacy in IoT environment. Data privacy is a matter that is closely related to the specification of data, the environment used to forward the data, and specifics about the content of the data. As IoT system mainly uses cloud environment for larger communication, hence, all the threats that are potential in cloud is also a matter of concern in IoT system. Securing larger number of connected physical devices using different protocols are quite challenging task. However, there are some deliberate attempts towards ensuring that highest form of data security over cloud. The brief discussion of the research contribution is as follows:

A. Data Security Schemes in IoT

The process of data security always calls for hiding the target data using different set of information or techniques as seen in majority of the patterns of research in IoT. There are studies to prove that image compression can be utilized for image security especially in IoT environment. The study carried out by Bezzateev and Voloshina [17] have shown that image compression technique using code-based approach can assists in better form of image encryption apart from benefit the storage size. An error-correcting codes was used for constructing error distribution blocks action as an encrypted image. There are also studies that offer enriched discussion of need of security over IoT in healthcare units. The study carried out by Kocabus et al.[18] discussed about presence of multiple layers of processes in IoT system. According to the authors, the threats imposed by side channel attacks are mainly resisted by public key encryption techniques inspite of their reported limitations [19].

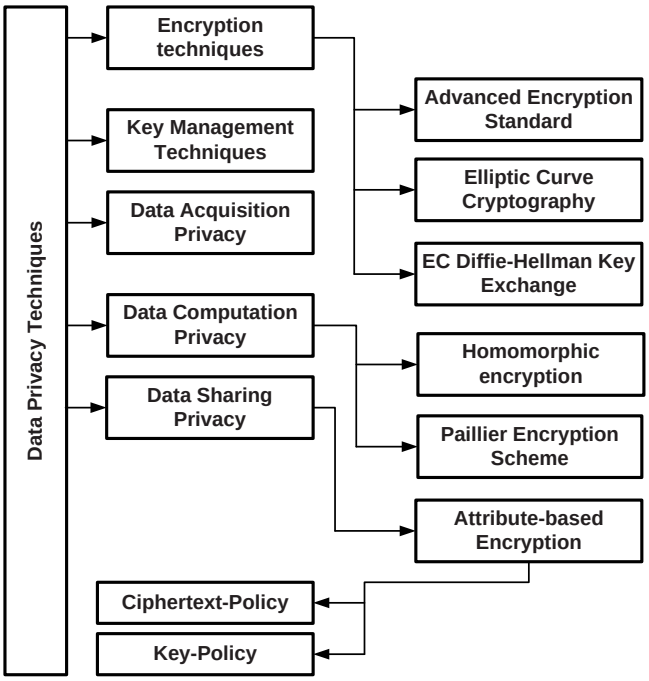


Fig. 1.Taxonomies of Data Security in IoT (Kocabus et al.[18])

Figure 1 highlights various forms of techniques on data security reported by existing researchers. It was also observed from the existing literature that IoT has been much proliferated in healthcare sector for assisting in various data aggregation process. Therefore, it also results in potential threat to patient's information. Usage of distributed source coding technique was proven to countermeasure such forms of threats on data security. Such study was carried out by Luo et al. [20]

by evolving up with a framework where the sensitive data of patient are aggregated from IoT devices as well as sensors and then stored in encrypted via secret shares form in the distributed cloud server. A non-conventional encryption mechanism was also researched in existing system in order to offer data security. Researchers such as Meng et al. [21] have developed a unique encryption scheme that uses sliding window concept as well as Merkle tree mechanism in order to offer encryption towards cloud data. Study towards data hiding was also carried out by Sharma et al. [22] considering the case study of healthcare. Perez et al. [23] have used symmetric encryption scheme using attribute-based scheme for improving the security while accessing resources over IoT devices. Most recently, the potential of blockchain mechanism is harnessed in offering data security on cloud-based operations [24]-[27]. Adoption of blockchain was proven to resist the threats on gateway protocol over IoT devices as reported by Cha et al. [28]. The mechanism calls for a specific enrolment process of the device administrator followed by constructing a blockchain network and its associated development of secure relationship with the gateway administrator. The authors have also used digital signature for further securing the encryption process. However, blockchain is fairly a new concept and will take a long period of time to evolve up with a benchmarked model in IoT

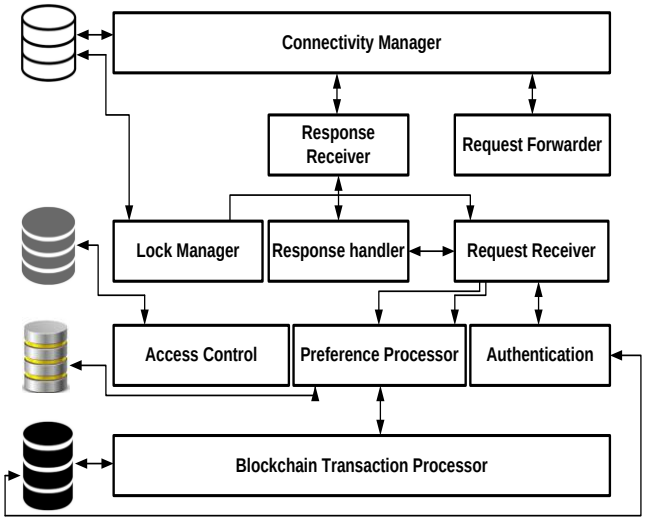


Fig. 2.Idea of Blockchain enabled gateway system [Cha et al. [28]]

B. Data Security Schemes in Cloud

The review of existing study was carried out over cloud security systems too as there are IoT system uses cloud as dependable communication environment. Studies e.g. [29]-[31] have emphasized on data security over cloud environment; however, this discussion will be narrowed towards considering image as a data. The study carried out by Abdul et al. [32] have utilized watermarking scheme in order to secure the ownership of an image. The study also advocates about the usage of visual encryption scheme that is capable of generating various secret shares without any adverse effect on resolution of original image. This scheme is normally assessed using visual quality and has been found to be extensively used by other researchers too e.g. [33]. The generic methodology adopted by all these researchers using visual encryption is pictorially shown in Fig.3.

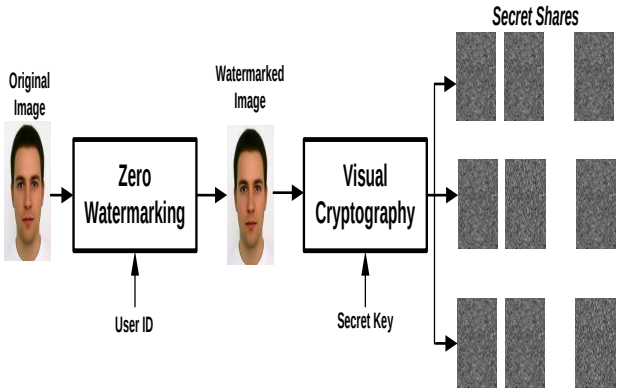


Fig.3. Process of Visual encryption scheme (Abdul et al. [32])

Encryption approach has been widely used for hiding the original image. A simplified encryption technique is also realized by involving non-complex techniques. The work carried out by Liang et al. [34] has used a clustering approach for performing encryption of image over cloud environment. The authors have implemented tree-based technique as well as histogram for performing encryption to offers better search time. The encryption operation over image is also improved by applying watermarking principle. The works of Liu et al. [35] have presented a security protocol that performs forwarding and retrieval of an encrypted watermarked image using hamming distance code and homomorphic encryption. The study outcome shows agreeable tolerance range but it lacks any form of comparative analysis. Usage of homomorphic encryption scheme was also reported by Yang et al. [36] where the encryption was applied directly to the pixels. The performance of image encryption can be further improved upon using histograms (Xu et al. [37]). The illegitimate change in histogram is best mechanism to identify the attack event.

C. Image Security Schemes in IoT

There are very much less reported works towards securing image in IoT environment; hence, only few literatures are explored in this category. It was noticed that hashing mechanism was used for safeguarding privacy factor of the image (Abduljabbar et al.[38]). Hardware-based approach was also seen to be adopted for improving the image security over IoT. Research in this direction has been carried out by Boutros et al. [39] and Omrani et al. [40] where the chaos theory was found to improvise image encryption. Most recently, an integrated encryption technique has been presented by Elhoseny et al.[41], where different forms of transformation technique has been used for encrypting medical images. There are also unique studies where image quality can be considered for extracting depth information in IoT. Such process can significantly improve the access rights on images stored over IoT devices (Liu et al. [42]). Study towards trust-based approach was carried out by Mohanty et al. [43], where a compression algorithm is utilized along with encryption and watermarking to offer better image security in IoT application.

Usage of probabilistic image encryption was seen in the work of Muhammad et al. [44] where the technique of hiding was discussed.

Similar mechanism of steganography was also discussed by Yin et al. [45]. Apart from this, it was observed that there are many researchers investigation data hiding problems in IoT using reversible data hiding techniques. However, majority of the techniques have focused on strengthening the recovery process but very less on the data hiding policies. Hence, there is a significant improvement of signal quality found in usage of this technique but they still suffers from some major pitfalls. Table 1 summarizes the research contribution of existing system towards problems of data security over IoT.

Table 1 Summary of Research Contribution of Data Security in IoT

Author	Problem	Technique	Advantages	Limitations
Bezzateev and Voloshina [17]	Image security	Error correcting codes, compression	Non-cryptographic approach	Doesn't ensure backward secrecy
Luo et al. [20]	Data privacy	Construction of secret shares, signcryption, SHA3	Simplified approach	Computationally extensive
Meng et al. [21]	Data security	Encryption, Sliding, Merkle tree	Compatible with smaller IoT devices	Involves significant cost of computation
Sharma et al. [22]	Data Security	Conceptualized	Cost effective implementation	No extensive analysis
Perez et al. [23]	Data Security	Symmetric encryption	Consistent run time performance	Not resistive against key-based attacks
Cha et al. [28].	Data Security	Blockchain, digital signature	Enhance trust in IoT	Computational extensive
Abdul et al. [32]	Image security	Visual encryption, watermarking	Good for identification as well as security	Generates overheads for multiple shares
Liang et al. [34]	Image security	Balanced binary tree, HSV/DCT histogram	Reduced search time	No benchmarking
Liu et al. [35]	Image security	Watermarking, hamming distance, homomorphic	Simplified technique	Generates overhead in IoT network
Yang et al.[36]	Image security	Homomorphic	Applicable to colored images.	Increased runtime
Xu et al. [37]	Image security	Histogram-based	Zero error in image recovery	Not tested over colored image
Elhoseny et al.[41]	Image security	Integrated Algorithm (AES, RSA, DWT)	Good structural performance, highly reduced error	Narrowed scope of analysis conducted in heterogeneous IoT device
Mohanty et al. [43]	Image security	Trust, Compression	Better optimization	Not resistive against lethal attacks
Jiang et al. [46], Kim [47], Mathew [48], Puteaux [49][50]	Data Hiding	Reversible data Hiding, Block shifting, reed-Solomon	Better reversibility	Not tested over real-time images
Qian et al.[51][52]	Data Hiding	Reversible data Hiding	Progressive mechanism	Not tested over real-time images, include overhead

III. RESEARCH PROBLEM

After reviewing the work of the existing system in prior section, it can be seen that there are various research work carried out towards securing data over IoT application. Although, the existing research techniques has offered some potential benefits, but there are some significant pitfalls too that are require equal attention. This section briefs about the identified research problems:

- ***Unsynchronized Domain of Technologies***: It is widely known that cloud computing and IoT are not considered in effective manner as it should be based on upcoming futuristic applications. There is still a contradictory and vagueness in modelling adversaries in cloud and in IoT. Cloud offers a large network of internet connectivity that also offers connection to various physical systems (but it is not always necessary).Similarly, IoT may use cloud as well as other large network system. Because of this reason, it will become quite challenging to offer data security as generic attacker role cannot be defined because of this differences. These dependencies are not studied properly with respect to selection of encryption technique at present.
- ***Very Less work on Image Security*:** Although, there are some good deal of work in data security over cloud, but there was no concrete claim if it is going to work for images too. The information within an image is quite high and complex as compared to normal plain text data. Moreover, images are frequently used as a medium of data communication in IoT in many applications apart from healthcare. Another important point to observe is that IoT nodes do not have very high computational capability and hence execution of complex encryption algorithm cannot be expected for resisting lethal threats for very long period of time.
- ***No work towards securing Aadhar card in IoT:*** At present, there are various devices in rural place which takes the biometric traits of Aadhar card holder to authenticate them for relaying some priviledge services. Usually, such biometric traits are compared with the computational model that has repositories of Aadhar card in the form of an image. Hence, information borne in Aadhar cards is highly essential and requires utmost security.

Currently, there is no work at present that has addressed the security of Aadhar card or any such identification-based image information in IoT application.

- ***Computationally Complex Process*:** The existing studies on securing communication in IoT include all form of complex cryptographic algorithm or some other optimization technique to strengthen the data security. However, it is carried out by ignoring the fact that IoT involves a large connection among different number of physical devices with lot of complex networking protocols. It also involves resource allocation while attempting to offer security. The resource constraint of IoT devices as well as capability constraint of the networking aspect is least considered while performing data hiding scheme in existing system.
- ***Unsolved Problems in Frequently Exercised Protocols*:** From prior section, it can be seen that reversible data hiding has been used widely by various researchers toward image security in IoT system. Although, this technique offers lossless acquisition of recovered data, but it ignores the encryption robustness. At present, none of the existing schemes of reversible data hiding has improved the blocking performance apart from iterative mechanism of block shifting with uniformity. The existing indexing mechanism of reversible data hiding is highly vulnerable to any form of memory based attacks as it bears the direct connectivity with the data to be carried out. Apart from this, the most notable problem is that it doesn't offer immediate response and hence is definitely no resistive against denial of service attack over IoT application.

Therefore, such unique problems are addressed in proposed system with significant improvement over existing techniques of data security in IoT.

IV. RESEARCH METHODOLOGY

The prime purpose of the proposed system is to develop a robust mechanism of data security in vulnerable communication system of IoT. The study considers that image plays a significant role in the form of data and is frequently used for communication among various cyber-physical systems in IoT environment. The proposed study considers a case study of safeguarding the private information of Aadhar card. Fig.4 highlights the adopted process flow of the proposed system that is designed considering analytical research methodology.

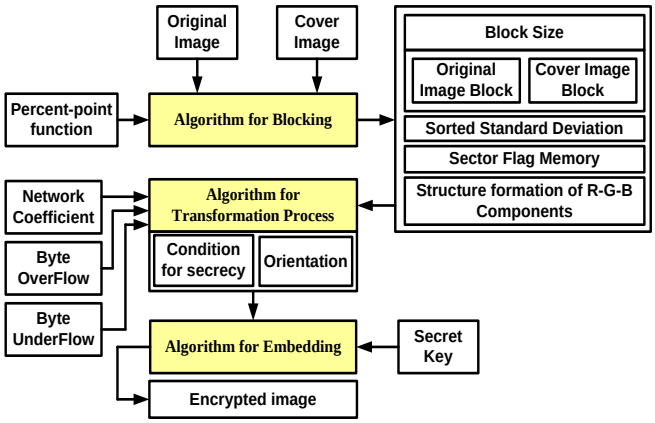


Fig.4. Process flow of Proposed System

The complete implementation process is divided into three discrete stages i.e. blocking stage, transformation stage, and embedding stage in order to hide the original image within a cover image. Unlike the conventional blocking, where blocking is carried out in simple and straight-forward manner, the proposed system offers a unique block processing operation. It applies blocking for both the images i.e. original as well as cover image and extracts statistical information in order to understand the discrete pattern of the given image. This discrete pattern is stored in the form of standard deviation and reposited over a unique actor of the study i.e. Sector Flag Memory. Basically, this is a memory system over the IoT device that is responsible for storing the random values for each individual blocks from source point (i.e. original image) to destination point (i.e. cover image). Interestingly, it only maintains length of the data and not the real data for which reason usage of Sector Flag Memory is very safer in contrast to any existing key management system practiced in cryptography approaches of IoT. The blocking operations results in generation of standard deviation of each color components whose random values are further processed for next process of transformation. The transformation process is carried out using network coefficient that represents network environment of IoT, and byte overflow/underflow parameters. The proposed transformation process also assists in executing secrecy condition as well as orientation process to ensure correct extraction of random patterns. Finally, a user-defined secret key is utilized for performing embedding operation of the original image over the cover image in order to obtain an encrypted image. Without usage of any complex or frequently used encryption scheme on image, the proposed system offers resistivity again many fatal threats. The next section elaborates about the algorithm design process.

V. ALGORITHM DESIGN

This section discusses about the strategies adopted for implementing the proposed algorithm that is essentially meant for data security in IoT application. The implementation of the algorithm mainly emphasizes data in the form of an image and hence applies the combination of image processing and encryption in order to achieve the objectives discussed in prior section. The complete process of algorithm implementation is discussed under two explicit categories of process of data hiding and extraction of data.

A. Data Hiding

The proposed system targets to safeguards the identity-based information of an individual that is retained in the form of an image. However, performing embedding operation of one image with other image may significantly result in perceptible image with artifacts. This challenge is addressed by introducing a simple and novel technique with series of algorithmic steps as discussed below:

i) Algorithm for Blocking

Although, there are various blocking operation carried out in past in medical image processing by various researchers, their motive of performing blocking was basically associated with granularity of information extraction.

Basically, a unique block of image can be considered as a partitioned sector that classified the complete image matrix with respect to some sizes say m *x* n. This virtual block is quite distinct in its size and is meant for completely overlay the actual image right from upper left corner with no possibilities of overlapping with each other. This operation leads to obtain user-defined size of blocks from the given input image where sampling and data extraction can be carried with better indexing. Extracting key features from one simple is always vague and ambiguous compared to same operation performed on different blocks of same image. The steps of the algorithm for performing blocking operation are as shown below:

Algorithm for Blocking
Input: I (original image), T (cover image), B_{size} (Blocking Size), τ (percent-point function)
Output: I_B /T_B (blocks of original and cover image)
Start
1. *init* I, T, $B_{size,}$ τ
2. I=p_{mxn} (I), T=p_{mxn} (T)
3. [(v_1 ix_1)(v_2 ix_2)]→sort (s(I_B, T_B))
4. Extract R_{comp}, G_{comp}, B_{comp}
5. **For** *k*=1:3
6. go to 2
7. (SI_B ST_B)→s(I_B, T_B))
8. update Line-3 w.r.t. SI_B and ST_B
9. **End**
10. obtain I_B, T_B
End

The illustration of the proposed algorithm is as follow: The algorithm basically takes two different types of input i.e. I (original image) and T (Cover image) that after processing leads the outcome of I_B /T_B (blocks of original and cover image) (Line-1). The algorithm also considers τ (percent-point function) as an input which is considered as a specific probability value that is always compared with certain specific probability limit in probability distribution (Line-1). This concept assists in understanding the sampling process in much better and faster way as the tentative value of τ (percent-point function) could be either more than or less than or equal to specific probability limit. This process offer faster block processing operation resulting in unique and non-redundant extraction of information from both the images. Inclusion of this process of percent-point function offers better construction of trap-door function. The implementation of the proposed block processing is carried out consider blocking size of 4 *x* 4. The next part of the algorithm implementation calls for enhancing the precision of both original I and cover image T to double (Line-2). In order to ease down the process of computation, the algorithm considers only grayscale image for processing, which will mean that the algorithm converts colored image to grayscale and then subject the grey scale image for further encryption process. All the image blocks after applying block processing results in rows and column wise blocks. The algorithm can thereby obtain the blocks of original image (I_B) and blocks of cover age (T_B) with respect to the initialized blocking size B_{size}. A statistical operation is carried out by applying a function *s* to compute standard deviation from both the blocks of an image i.e. I_B and T_B. The sorting of I_B and T_B is carried out using map-based parameters i.e. (v_1 ix_1) and (v_2 ix_2), where v_1 and v_2 represents standard deviation of original and cover image respectively (Line-3). The variables (ix_1 and ix_2) are considered as flags of the sorted matrix (Line-3). The algorithm than takes the input of user-defined value of percent-point function and initialize a new variable called as Sector Flag Memory (SFM) that are maintained in the form of sequences. The sequences of SFM is constructed by assigning a matrix of elements one with single row and columns of the size of (ix_1 or ix_2). This process generates two sequences i.e. SFM_1 and SFM_2. In the next process, all the initial value of the percent-point function is converted to 0 followed by applying reshaping operation. This process leads to generation of the blocks of both original and cover image.

However, the above mentioned process is only applicable when the image is gray scaled. Otherwise, the algorithm performs the task in slightly different manner. If the input image is found to be colored image, than a structure is constructed for blocks of cover image (I_{Bs}), block of cover image (T_{Bs}), structure of Sector Flag Memory (SFM_{1s} and SFM_{2s}). A new structure is constructed in order to reposit the red, green, and blue component (Line-4). Each 3 unique components are now subjected to following operation (Line-5):- The algorithm forms a column vector from the blocks of original and cover image that is directly implementing Line-2. The algorithm now assigns the blocks of original and cover image discretely to structures of them (i.e. I_{Bs} and T_{Bs}). The next part of implementation is to compute the standard-deviation of original image as well as cover image (Line-7). After sorting the obtained value of SI_B and ST_B, the further updated value of standard deviations (v_1 v_2) and flags (ix_1, ix_2) are obtained. The next operation further repeats the similar process of generation of two sequences of SFM_1 and SFM_2; however, this time it amends it with respect to the structure formed by the image blocks. Basically, the implementation of this algorithm results in two output viz. image (i) IB obtained from IB_s and TB obtained from TB_s) and data (i) SFM obtained from SFM_{1s} and ii) SFM_2 obtained from SFM_{2s}). However, as a visible outcome, I_B and T_B are core outcomes of this algorithm (Line-10).

ii) Algorithm for Transformation Process

This is basically an intermediate processing that takes place after the blocked images of original and cover image is obtained and before the process of embedding original to cover image. Hence, it is essential that this process is designed with utmost care because a slightest flaw will lead to incompatibility of the obtained blocked image to be subjected to encoding system. At the same time, it is required that a good forward and backward secrecy to be maintained while constructing the encoding process in order to offer safety from different vulnerable systems in IoT. The complete transformation process is implemented over the blocks that have been recently obtained in prior algorithm implementation. In order to carry out an effective transformation with retention of better secrecy mode, it is essential to ensure that the transformed image be obtained from both original as well as cover image. The proposed system considers standard deviation as well as SFM version of both original and cover image in order to obtain the transformed image.

It will also mean that transformed image is also of two types i.e. transformed image with standard deviation and SFM. The significant steps of the proposed algorithm are as follows:

Algorithm for Transformation Process

Input: μ (network coefficient), B_{size} (Blocking Size), β_{max} (byte overflow), γ_{min} (byte underflow)

Output: E_1 (Generation of Secret Image)

Start

1. init B_{size}, $\beta_{max,}$ γ_{min}
2. (I, T)=double (I, T)
3. f→*explore*(SFM==0)
4. (ix_1 ix_2)=ψf
5. **For** i=1:size(RSI_B)
6. (O_{B1}, T_{B1})→p(O_{B1}, T_{B1}, B_{size})
7. (op_{block}, ϕ, ρ)→f(O_{B1}, T_{B1}, μ, $\beta_{max,}$ γ_{min})
8. **End**
9. ρ →2.(ρ / μ)
10. E_I→f_1(T_{Bm})

End

The steps of the algorithm for transformation are as follows: The algorithm takes the input of λ (network coefficient), B_{size} (Blocking Size), β_{max} (byte overflow), and γ_{min} (byte underflow) that gives and outcome of E1 (Generation of Secret Image) (Line-1). The first step of the algorithm is to obtain few mapping parameters e.g. *r*, *c*, and *m* from original image I. This operation is followed by enhancing to double precision for both original image I and cover image T (Line-2) along with initialization of block size B_{size}. The transformation process also particularly emphasize on retaining higher degree of imperceptibility towards the encrypted image. A better form of imperceptibility can be only maintained if the algorithm ensures less or zero occurances of byte overflow and underflow of image pixels. The proposed system performs analysis with respect to different value of β_{max} (byte overflow) and γ_{min} (byte underflow). If the size of *m* is found to be unity than the algorithm captures the double precisive value of original image and cover image. The next step of the algorithm is to extract the flag information (ix_1 ix_2) from the sequences of SFM (i.e. SFM_1 and SFM_2) (Line-3). This execution process calls for exploring all the respective values where 4 different values will be extracted i.e. a_1=*explore*(SFM_1=0), a_2=*explore*(SFM_2=0), a_3=*explore*(SFM_1), a_4=*explore*(SFM_2). The flag values f is obtained as ix_1→(a_1 a_2) and ix_2→(a_3 a_4) (Line-3). All these operations are carried out by a discrete function ψ (Line-4). The next process is to perform rearrangement of the blocks. For this purpose, two blocks RSI_B and RTI_B is formed that represents rearranged blocks for original image and cover image that considers all the row elements; however, it column elements considered are flag elements ix_1 and ix_2 respectively for RSI_B and RTI_B. The optimal direction vector ϕ is initialized as a matrix with a size equivalent to that of RSI_B and ρ represents difference between the average value of final block and original block. The dimension of the ρ is equal to that of RSI_B. Hence, for all the values of RSI_B (Line-5), the original block and the targeted block are obtained from RSI_B and RTI_B respectively (Line-6). The algorithm finally applies block processing operation in order to obtain numerical outcome of optimized block *opblock*, optimal direction vector ϕ, and ρ (Line-7). The final computation of ρ is carried out (Line-9) using a network coefficient μ. Finally, the transformed image EI is obtained by applying function f_1(x) that takes the unique columnar elements from optimized block *opblock*. The complete process results in generation of secret image.

iii) Algorithm for Embedding

Embedding the original image within a coverage is highly important operation of image security to ensure that the resultant image i.e. target image should not look different than cover image i.e. good imperceptibility. In case the target image is found to be look differently than the cover image that it could offer a possible hint to the attacker about the image security approaches being used to hide the original image. Hence, development of this algorithm is carried out considering usage of very simplistic encoding scheme that could significantly balance byte overflow/underflow in order to hide any form of traces or artifacts. This algorithm is responsible for performing embedding operation and its steps are as follows:

Algorithm for Embedding

Input: E_I (Secret Image)

Output: T_{im} (Target Image)

Start

1. [*r c m*]→size(E_I)
2. E_I→f_3(E_I)
3. if *m*==1
4. ϕ_b→*enc*(ϕ_b -1)
5. ρ_b→*enc*(ρ)
6. $data_{tot}$→(ϕ_b, ρ_b)
7.. $data_{tot}$→ $data_{tot}$(R_{ix})
8. T_{im}→enc(f_3(E_I))
9. **End**

End

The description of the algorithmic steps are as follows: In the initial steps, the algorithm takes the input of secret image E_I, whose size information is extracted and mapped into three variables *r*, *c*, and *m* (Line-1). It applies a function f_3(x) that applies double precision to the unsigned integer of 8 bits to the secret image E_I (Line-2). With a condition that *m* is equivalent to unity (Line-3), the proposed system computes updated directional vector ϕ_b by applying simple encoding operation *enc* over (ϕ_b-1) (Line-4). Similarly, the algorithm also computes the updated average difference ρ_b by similar encoding procedure over prior value of average difference (Line-5). The cumulative data to be subjected to the embedding process is actually dependent on three parameters, sector flag memory, direction vector, and average difference (Line-6). The study uses a secret key that is fed by the user itself. After the user feeds the secret key, it performs random permutation of the length of the total data to be embedded and stored in variable R_{ix} (Line-7). Hence, the matrix $data_{tot}$ actually contains information about the length of the cumulative data and not the actual data. The next process is further applying similar function f_3(x) on E_I (Line-8) followed by similar encoding operation to obtain the finally a target image. Basically, this image consists of a cover image within which the original image is hidden within. The target image is visually similar to cover image as well as it also offers nearly similar numerical resolution corresponding to the cover image.

The next section discusses about the results being accomplished from the proposed system implementation.

Table 2 Essential Notations used

I	original image
T	cover image
T_{im}	Target Image
E_I	Secret Image
B_{size}	Blocking Size
τ	percent-point function
I_B /T_B	blocks of original and cover image
μ	network coefficient
β_{max}	byte overflow
γ_{min}	byte underflow
p	resizing /reshaping function
s	standard deviation
v_1/v_2	standard deviation of original/cover image
ix_1/ix_2	flag of original/cover image
ϕ	Direction vector

b) Data Recovery

The process of data recovery is mainly associated with the decryption or decoding process in order to gain an access to the original data or image. This process of decryption is strongly dependent on the secret key that was used by the user during the encryption or embedding process. The input to the data recovery process is basically the outcome of algorithm for embedding i.e. targeted image or encrypted image where the original image is hidden on the background while cover image resides on the foreground. The input to the data recovery process is encrypted image. After the encrypted image has been selected, the next operation is all about extracting the hidden data i.e. original image. For this purpose, same key used during encryption are used as well as similar block size is given. The size of the encrypted image is extracted after converting it to double precision. The prime operations involved during the decryption process are:

- ***Computation of length of Sector Flag Memory (SFM).*** This is computed by dividing the product of *r* and *c* by square of the block size B_{size}. The variable r and c represents the rows and columns of the double precision encrypted image T_{im}.
- ***Computation of length of direction vector (ϕ)*:** The process computes the length of ϕ using similar empirical mechanism with minor change. The value of length of ϕ is obtained by dividing twice the value of product of *r* and *c* with square of block size B_{size}.
- ***Computation of length of average difference (μ)*:** The value of length of μ is obtained by dividing six times the value of product of *r* and *c* with square of block size B_{size}.

All the above information are added in order to obtain the final length of data. The similar encoding function *enc* is applied to the T_{im} considering only 8 bits of data at a time and the obtained data is stored in temporary matrix. The consecutive process extracting SFM, direction vector, and average difference from inverse permutation of secret key over obtained encrypted value. Reverse decoding function *dec* is applied to recover all the above three dependencies as updated form and finally successful extraction of original image I is carried out at the end. One interesting fact about this recovery process is that even if the encrypted image falls in the captivity of the attacker, owing to multiple dependencies it is extremely challenging for attacker to break the code. Such computations of those dependencies are also dependent of random parameters as well as unique mode of operation, which is out of scope for attacker to possess the knowledge. Hence, the proposed algorithm constructs a good trap-door function with robust forward and backward secrecy for image security.

VI. RESULT ANALYSIS

The implementation of the proposed study was carried out on real-time images of Aadhar card of more than 50 different human subjects. The images of the Aadhar card and the corresponding human subjects were captured using digital camera of 20 megapixel resolution. Fig.5 highlights only 3 samples of it (the prominent information of subject's visual identity are hidden in this in order to safeguard the privacy).

i) Visual Outcome Analysis

All the analysis was carried out considering colored images with different dimensions as shown in Fig.5.

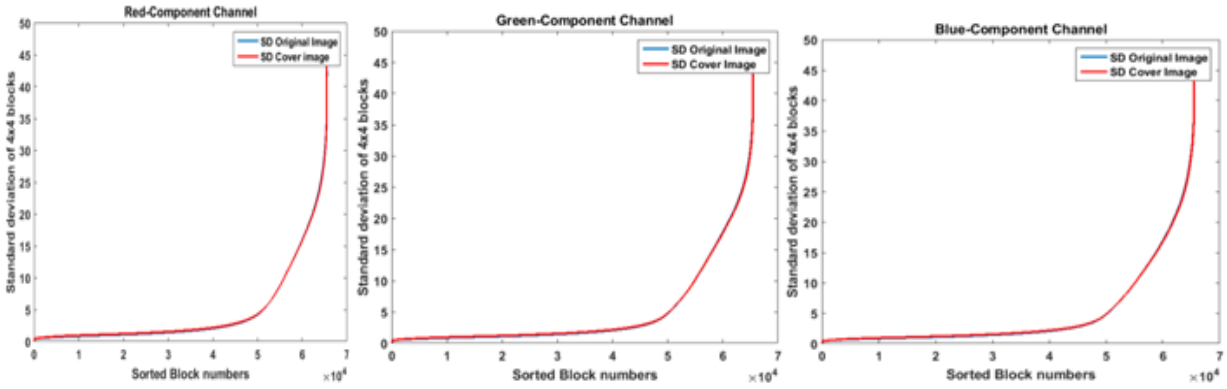
Subject-3

Dimension: 2064 x 1878

(a) Original Image **b) Cover Image**

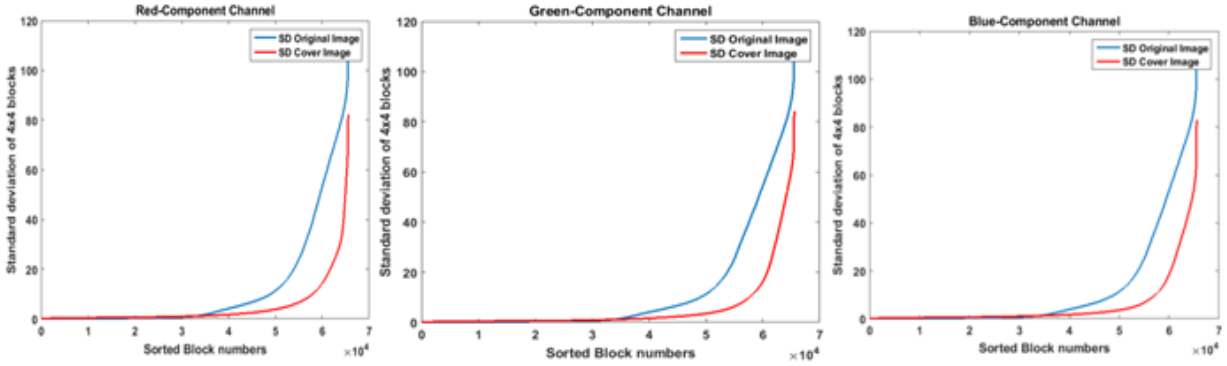
Fig.5 Visuals of Input Considered in Proposed Experiment

Although, the visuality of Aadhar card is same for everyone with one format to represents the identity, the inputs of original images are not kept uniform intentionally. For an example, a closer look into Aadhar card of subject-1 will show that there is less than 10^{o} of tilt while that of subject-3 has approximately 30^{o} of tilt. On the other side, subject-2 has 0^{o} tilt. Same principle goes for cover images too. The prime reason behind this is majority of the existing system make use of templates for perform [53]-[54]. Hence, attack on images on such template-based approach makes vulnerable to collateral images. As if one template's orientation is disclosed, all other images become vulnerable to be compromised. Also, it is not necessary to retain same subject's image in cover page, it could be any random image too. However, for better identification in the decryption process, it is recommended to use the image of original and corresponding subjects. Hence, the system takes the input of both original image and cover image and continues with blocking operation of 4x4. The proposed system carryout blocking operation considering standard deviation of percent-point function τ value to be residing within 20-90 percentile scale. This process performs analysis of standard deviation of red-green-blue components.



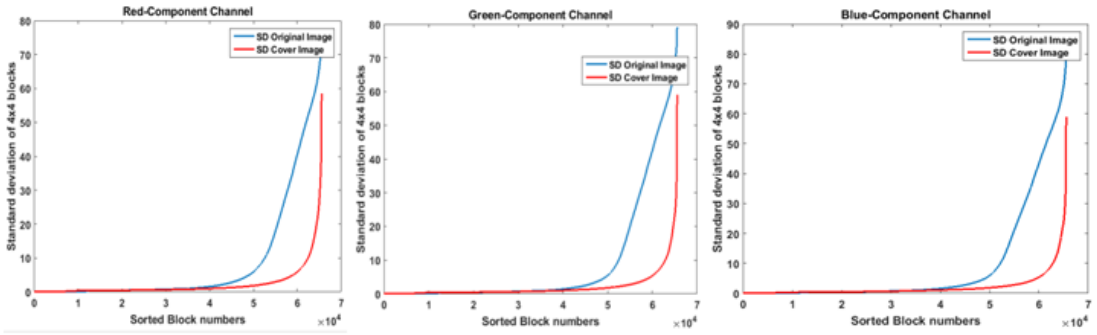
(a) Red-Component **(b) Green-Component** **(c) Blue Component**

Fig. 6. Analysis of Standard Deviation of R-G-B Components for Subject-1



(a) Red-Component **(b) Green-Component** **(c) Blue Component**

Fig.7. Analysis of Standard Deviation of R-G-B Components for Subject-2



(a) Red-Component (b) Green-Component (c) Blue Component

Fig.8. Analysis of Standard Deviation of R-G-B Components for Subject-3

The Figure 6-8 highlights the standard deviation of three different subjects to show that there is a unique pattern of standard deviation for original image and cover image of all the three sample human subjects. The outcomes are obtained by blocking both the original and cover image in the scale of 4*x*4. This outcome could also be interpreted as following- there are various existing approaches e.g. [56] that claims of considering extracting unique pattern of image in the form of feature-based approach using diversified techniques. Compared to any such featured-based image encryption techniques, the proposed system only makes use of descriptive statistical parameter i.e. standard deviation to represent such feature/pattern of both original image and cover image. The output of all the above graphs are obtained by executing first algorithm of blocking in order to achieve the results of sorted standard deviation of original image (v_1) and cover image (v_2). The proposed technique offer much faster mechanism of extracting the standard deviation of the red-green-blue components very discretely with increasing number of image block. This is a very simplified steps as well as very novel step that doesn't involve in increase any form of computational overhead to adversely affect the image quality at the end. The benefit of this scheme can be realized by computing the algorithm processing time for blocking and transformation process involved in both existing system and proposed system.

ii) Validation Analysis

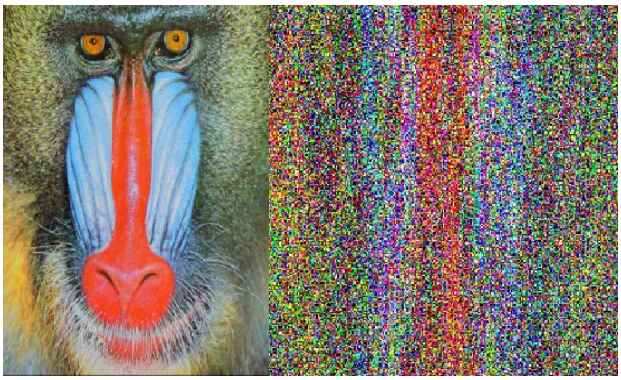
The validation of the proposed prototyped scripted in MATLAB was tested with more than 100 number of original and cover images. The analysis was carried out with different combination of considering correct / incorrect version of images as well as secret keys. Following are the respective visual outcomes.

(a) Encrypted Image (b) Retrieved image

Fig. 9. Validation with Correct Encrypted image & Incorrect Secret Key

(a) Encrypted Image (b) Retrieved image

Fig.10. Validation with Incorrect Encrypted image & Correct Secret key



(a) Encrypted Image (b) Retrieved image

Fig.11. Validation with Incorrect Encrypted image & Incorrect Secret key

All the visual outcomes are assessed while considering input of encrypted image only during the process of data recovery. Figure 9 and Figure 11 shows that consideration of incorrect key with correct / incorrect encrypted images results in completely corrupted image as a retrieved data. Otherwise, selection of correct secret key and incorrect encrypted image file (Figure 10) will result in random images (that can be also considered as cheat images essentially mean for invoking obfuscation to the attackers). This outcome shows that secret key is one prominent dependency to obtain retrieved images or else it starts offering cheat images. Hence, the proposed system offers robust obstruction to attacker to maliciously access any encrypted data.

iii) Comparative Analysis

There are various research work carried out in past that has adopted reversible encryption technique e.g. [46]-[51]. Although, the baseline methodology of the proposed system is also based on similar approach, but the proposed study incorporates its algorithms to induce higher degree of forward-backward secrecy as well as quite independent of complex key management strategies unlike existing system. Hence, for comparative analysis, the proposed system implements the standard logic of reversible data hiding scheme and consider it as *Existing System* in Table 2 and Table 3 while *Proposed* refers to implementation of algorithms discussed in this paper. The analysis was carried out with respect to algorithm processing time that is further classified in the form of Embedding time and Decryption Time. The study also checks for Peak Signal-to-Noise Ratio (PSNR) for assessing the visual quality.

Table 2 Comparative Analysis of Encryption Time

	Encryption	Embedding Time	PSNR
Subject-1	Existing	333.813	53.1839
	Proposed	69.7615	53.1839
Subject-2	Existing	348.1938	53.1792
	Proposed	69.5311	53.1792
Subject-3	Existing	332.5621	53.2219
	Proposed	69.8427	52.2219

Table 3 Comparative Analysis of Decryption Time

	Decryption	Recovery time
Subject-1	Existing	1.19
	Proposed	1.01
Subject-2	Existing	1.25
	Proposed	0.62
Subject-3	Existing	1.32
	Proposed	0.92

The numerical outcome clearly shows that proposed system takes considerably very lesser amount of algorithm processing time as compared to the existing approaches of data encryption. The embedding time is usually higher compared to decryption time, which is quite normal in both the cases, but proposed system offers lesser consumption of decryption time as it works completely on statistical computation that is not only faster but also accurate. However, signal qualities of both the system are quite similar. The implementation of the algorithm completely focuses on minimizing recursive steps of encryption that is necessary for offering faster response time. Adoption of directional vector, average difference, sector flag memory, and percent-point function are some definitive implementation that offers higher degree of reduction of encryption effort and other unnecessary dependencies, unlike existing system.

iv) Security Strength Analysis

A closer analysis towards any forms of attacks in IoT system shows that presences of malicious code are primarily responsible for initiating attacks. The attacks are mainly towards node that posses the secret key in certain physical environment. The proposed mechanism doesn't retain secret keys anywhere in the entire physical environment and hence it is free from any *key-based attacks*. Another significant benefit is usage encryption is performed over the length of the cumulative data and not over the actual data. This makes the process free from direct access to any data that normally happens during the state of *Denial-of-Service* attack in IoT. Finally, the proposed system uses a mechanism of SFM that retains information about specific flag which is just an abstraction of memory of original image and not completely original image and hence it is free from any *memory-based attacks*.

VII. APPLICATIONS

The design of the application depends on utility of Aadhar card in existing as well as futuristic system. It is also known that existing m-commerce as well as e-commerce application, requires true identification of their users whether it is vendor or buyer. In this case if Aadhar card is considered to be used for online identity-based authentication, it is required to be stored in some place for which reason it will call for executing proposed data security discussed in this book chapter. Fig.12 highlights the possible application scenario of proposed system.

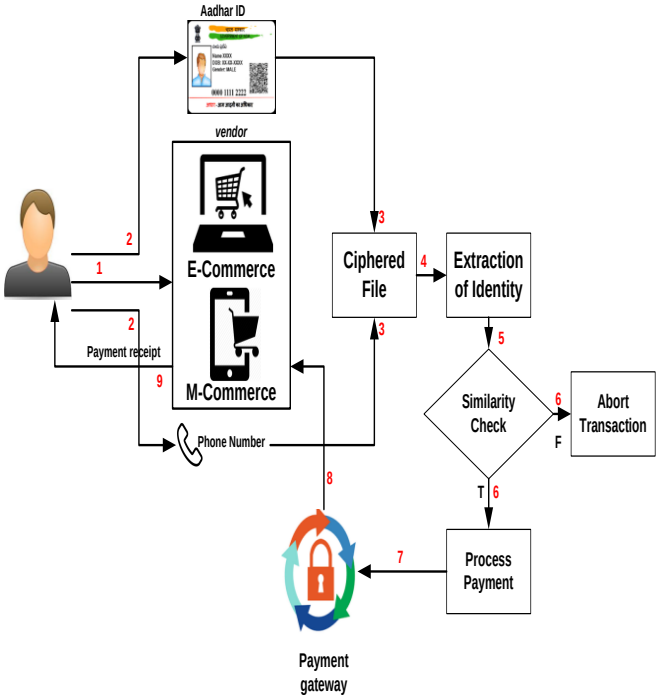


Fig.12. Possible Application scenario of proposed system

According to the possible application, the user will be required to store the Aadhar card in the secure server over IoT networks. The next process is to access the stored Aadhar card by executing the proposed algorithm that will finally generate a ciphered file. The ciphered file will be constructed on the basis of stored image of Aadhar card and a phone number or anything else that will be treated as a cover image. The next process is all about extraction of legitimate identity of the user that will be undergoing a similarity check with that stored database of vendor. In case of illegitimate image entry, the transaction will be aborted otherwise the transaction will be proceeded to the payment gateway system to complete the transaction process. At present, there is no commercial application that performs image-based security checks like the proposed technique and hence is a novel concept of data security over an IoT environment.

VIII. CONCLUSIONS

The proposed system is design to offer a robust data security to the unique identification system called as Aadhar card using image processing concept. The significant contribution of the proposed system are i) it is completely independent of any form of complex encryption technique, ii) it offers good balance between forward and backward secrecy, iii) the computational processing speed of proposed system is found to be extensively faster in contrast to frequently used reversible data hiding techniques, iv) it is also resistive against multiple security problems e.g. denial-of-service, key-based attacks, and memory-based attack. The future work will be continued in the direction of further optimizing the embedding scheme.

REFERENCES

1. Vladimir Hahanov, Cyber Physical Computing for IoT-driven Services, Springer-technology, 2018
2. Olof Liberg, Marten Sundberg, Eric Wang, Johan Bergman, Joachim Sachs, Cellular Internet of Things: Technologies, Standards, and Performance, Academic Press, Technology &Engineering, 2017
3. Chong-Min Kyung, Hiroto Yasuura, Yongpan Liu, Smart Sensors and Systems: Innovations for Medical, Environmental, and Iot Applications, Springer Customer Service Center, 2018
4. Hiroto Yasuura, Chong-Min Kyung, Yongpan Liu, Youn-Long Lin, Smart Sensors at the IoT Frontier, Springer, technology &Engineering, 2017
5. Shancang Li, Li Da Xu, Securing the Internet of Things, Syngress, Computer, 2017
6. Brian Russell, Drew Van Duren, Practical Internet of Things Security, Packt Publishing Ltd, 2016
7. M. Azarmehr, A. Ahmadi and R. Rashidzadeh, "Secure authentication and access mechanism for IoT wireless sensors," *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*, Baltimore, MD, 2017, pp. 1-4.
8. S. Batool, N. A. Saqib and M. A. Khan, "Internet of Things data analytics for user authentication and activity recognition," *2017 Second International Conference on Fog and Mobile Edge Computing (FMEC)*, Valencia, 2017, pp. 183-187.
9. H. Kim and E. A. Lee, "Authentication and Authorization for the Internet of Things," in *IT Professional*, vol. 19, no. 5, pp. 27-33, 2017.
10. O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab and A. Kayssi, "Identity-based authentication scheme for the Internet of Things," *2016 IEEE Symposium on Computers and Communication (ISCC)*, Messina, 2016, pp. 1109-1111.
11. J. Dofe, J. Frey and Q. Yu, "Hardware security assurance in emerging IoT applications," *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*, Montreal, QC, 2016, pp. 2050-2053.
12. J. Chauhan, S. Seneviratne, Y. Hu, A. Misra, A. Seneviratne and Y. Lee, "Breathing-Based Authentication on Resource-Constrained IoT Devices using Recurrent Neural Networks," in *Computer*, vol. 51, no. 5, pp. 60-67, May 2018.
13. A. Joshy and M. J. Jalaja, "Design and implementation of an IoT based secure biometric authentication system," *2017 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES)*, Kollam, 2017, pp. 1-13.
14. https://www.uidai.gov.in/
15. M. Zhou, R. Zhang, W. Xie, W. Qian and A. Zhou, "Security and Privacy in Cloud Computing: A Survey," *2010 Sixth International Conference on Semantics, Knowledge and Grids*, Beijing, 2010, pp. 105-112.
16. R. Mathur, S. Agarwal and V. Sharma, "Solving security issues in mobile computing using cryptography techniques — A Survey," *International Conference on Computing, Communication & Automation*, Noida, 2015, pp. 492-497.
17. Bezzateev, Sergey, and Natalia Voloshina. "Image encryption in code based compression algorithms based on multilevel image structure model." Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2017 9th International Congress on. IEEE, 2017.
18. Kocabas, Ovunc, Tolga Soyata, and Mehmet K. Aktas. "Emerging security mechanisms for medical cyber physical systems." IEEE/ACM transactions on computational biology and bioinformatics 13.3 (2016): 401-416.
19. X. Zhang, C. Xu, R. Xie and C. Jin, "Designated Cloud Server Public Key Encryption with Keyword Search from Lattice in the Standard Model," in *Chinese Journal of Electronics*, vol. 27, no. 2, pp. 304-309, 3 2018.
20. Luo, Entao, et al. "PrivacyProtector: Privacy-Protected Patient Data Collection in IoT-Based Healthcare Systems." IEEE Communications Magazine 56.2 (2018): 163-168.
21. Meng, Qian, et al. "Comparable Encryption Scheme over Encrypted Cloud Data in Internet of Everything." Security and Communication Networks 2017 (2017).
22. Sharma, Sagar, Keke Chen, and Amit Sheth. "Toward practical privacy-preserving analytics for iot and cloud-based healthcare systems." IEEE Internet Computing 22.2 (2018): 42-51.
23. Pérez, Salvador, et al. "A lightweight and flexible encryption scheme to protect sensitive data in Smart Building scenarios."IEEE Access (2018).
24. C. Xu, K. Wang and M. Guo, "Intelligent Resource Management in Blockchain-Based Cloud Datacenters," in *IEEE Cloud Computing*, vol. 4, no. 6, pp. 50-59, November/December 2017.
25. C. Esposito, A. De Santis, G. Tortora, H. Chang and K. K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," in *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31-37, Jan./Feb. 2018.
26. H. Liu, Y. Zhang and T. Yang, "Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing," in *IEEE Network*, vol. 32, no. 3, pp. 78-83, May/June 2018.
27. P. K. Sharma, M. Y. Chen and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," in *IEEE Access*, vol. 6, pp. 115-124, 2018.
28. Cha, Shi-Cho, et al. "A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things." IEEE Access 6 (2018): 24639-24649.
29. P. Li, S. Guo, T. Miyazaki, M. Xie, J. Hu and W. Zhuang, "Privacy-Preserving Access to Big Data in the Cloud," in *IEEE Cloud Computing*, vol. 3, no. 5, pp. 34-42, Sept.-Oct. 2016.
30. P. Zhang, J. K. Liu, F. R. Yu, M. Sookhak, M. H. Au and X. Luo, "A Survey on Access Control in Fog Computing," in *IEEE Communications Magazine*, vol. 56, no. 2, pp. 144-149, Feb. 2018.
31. V. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," in *IEEE Transactions on Services Computing*, vol. 9, no. 1, pp. 138-151, Jan.-Feb. 1 2016.
32. Abdul, Wadood, et al. "Biometric security through visual encryption for fog edge computing." IEEE Access 5 (2017): 5531-5538.
33. U. H. Panchal and R. Srivastava, "A Comprehensive Survey on Digital Image Watermarking Techniques," *2015 Fifth International Conference on Communication Systems and Network Technologies*, Gwalior, 2015, pp. 591-595.
34. Liang, Haihua, et al. "Secure and Efficient Image Retrieval over Encrypted Cloud Data." Submitted To Security And Communication Networks, 2017
35. Liu, Keyang, Weiming Zhang, and Xiaojuan Dong. "A Cloud-User Protocol Based on Ciphertext Watermarking Technology." Security and Communication Networks 2017 (2017).
36. Yang, Pan, et al. "An Efficient Secret Key Homomorphic Encryption Used in Image Processing Service." Security and Communication Networks 2017 (2017).
37. Xu, Dawen, et al. "Separable Reversible Data Hiding in Encrypted Images Based on Two-Dimensional Histogram Modification." Security and Communication Networks 2018 (2018).
38. Abduljabbar, Zaid Ameen, et al. "Privacy-preserving image retrieval in IoT-cloud." Trustcom/BigDataSE/I SPA, 2016 IEEE. IEEE, 2016.
39. Boutros, Andrew, et al. "Hardware acceleration of novel chaos-based image encryption for IoT applications." Microelectronics (ICM), 2017 29th International Conference on. IEEE, 2017.
40. Omrani, Tasnime, et al. "RARE: A robust algorithm for rapid encryption." Internet Technology and Secured Transactions (ICITST), 2017 12th International Conference for. IEEE, 2017.
41. Elhoseny, Mohamed, et al. "Secure medical data transmission model for IoT-based healthcare systems." IEEE Access 6 (2018): 20596-20608.

42. Liu, Xingang, et al. "Joint 3-D image quality assessment metric by using image view and depth information over the networking in IoT." IEEE Systems Journal 10.3 (2016): 1203-1213.
43. Mohanty, Saraju P., Elias Kougianos, and Parthasarathy Guturu. "SBPG: Secure Better Portable Graphics for Trustworthy Media Communications in the IoT." IEEE Access6 (2018): 5939-5953.
44. Muhammad, Khan, et al. "Secure Surveillance Framework for IoT systems using Probabilistic Image Encryption." IEEE Transactions on Industrial Informatics (2018).
45. Yin, Joanne Hwan Jie, et al. "Internet of Things: securing data using image steganography." Artificial Intelligence, Modelling and Simulation (AIMS), 2015 3rd International Conference on. IEEE, 2015.
46. Jiang, Ruiqi, et al. "A High-Capacity Reversible Data Hiding Method in Encrypted Images Based on Block Shifting." 2017 2nd International Conference on Multimedia and Image Processing (ICMIP). IEEE, 2017.
47. T. Kim and S. Kim, "Efficient Transmission of Reversible Data Hiding in Encryption Images by Using Reed-Solomon Codes," *2015 3rd International Conference on Future Internet of Things and Cloud*, Rome, 2015, pp. 765-769.
48. T. Mathew and M. Wilscy, "Reversible data hiding in encrypted images by active block exchange and room reservation," *2014 International Conference on Contemporary Computing and Informatics (IC3I)*, Mysore, 2014, pp. 839-844.
49. P. Puteaux and W. Puech, "An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1670-1681, July 2018.
50. Puteaux, Pauline, and William Puech. "Reversible data hiding in encrypted images based on adaptive local entropy analysis." Image Processing Theory, Tools and Applications (IPTA), 2017 Seventh International Conference on. IEEE, 2017.
51. Z. Qian, H. Xu, X. Luo and X. Zhang, "New Framework of Reversible Data Hiding in Encrypted JPEG Bitstreams," in *IEEE Transactions on Circuits and Systems for Video Technology*
52. Qian, Zhenxing, Xinpeng Zhang, and Guorui Feng. "Reversible data hiding in encrypted images based on progressive recovery." IEEE signal processing letters 23.11 (2016): 1672-1676.
53. A. Selwal, S. K. Gupta, Surender and Anubhuti, "Performance analysis of template data security and protection in Biometric Systems," *2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS)*, Chandigarh, 2015, pp. 1-6.
54. A. Ross and A. Othman, "Mixing fingerprints for template security and privacy," *2011 19th European Signal Processing Conference*, Barcelona, 2011, pp. 554-558.
55. S. S. Shen, T. H. Kang, S. H. Lin and W. Chien, "Random graphic user password authentication scheme in mobile devices," *2017 International Conference on Applied System Innovation (ICASI)*, Sapporo, 2017, pp. 1251-1254.

AUTHORS PROFILE

Chhaya S Dule is working as Associate Professor in the Department of Computer Science and Engineering, KG Reddy College of Engineering & Technology, Hyderabad, Telangana-State, India. She is pursuing her Ph.D in Computer Science and Engineering from Visvesvaraya Technological University, Belgaum. She has completed her B.E from Shri Guru Gobind Singhji College of Engineering, Nanded (Dr. Babasaheb Ambedkar Aurangabad University) and M.Tech in Computer Science and Engineering from Samrat Ashok Technological Institute Vidisha (Rajiv Gandhi Proudyogiki Vishwavidhyalaya, Bhopal). She is having 17+ years of Teaching experience. Her domain area of research is Cloud Computing - Security Issues. Her other area of interest are DBMS, Software Engineering , Software Testing, Big Data Analytics , Data Mining and Data Warehousing , Neural Network and Fuzzy logic. She has research publications in reputed National and International journals. She has published 9 international research paper and 11 national papers in various conferences and journals. She has attended 4 faculty development programs (FDP) organized by AICTE and TEQIP and 8 workshops on various topic. She is Life Member of CSI and ISTE professional bodies.

Dr. Nandini N, Currently She is working as associate Professor in the department of CSE in Dr. Ambedkar Institute of Technology, Bengaluru, India. She has published papers in international and national journals & conferences. She is having more than 10 years of work experience in academic.

Dr. Rajasekharaiah K.M. is working as Dean & Professor, Faculty of Information Technology, AMITY Institute of Higher Education, Mauritius. He has done B.E, M.Tech in Computer Science & Engineering, M.Phil. in Computer Science, from reputed Universities, India. He is having 32+ years of total experience including 18 years of Industrial and remaining Teaching experiences. He is a Life fellow Member of Indian Society for Technical Education (ISTE), New Delhi. He has completed his PhD in the domain area of Data Mining & Data Warehousing. He has research publications in reputed National and International journals. His other area of interests is DBMS, Software Engineering, Software Architecture, Computer Networks, Data Structures and Mobile Computing. Further, he has served as Vice Principal, Director – Academics, Dean – R & D, Coordinator for NBA and NAAC accreditation process and presentation in Engineering Colleges. He organized and participated in Conference, Seminars, Workshops and FDPs at various National and International levels.